

# H3C 无线控制器典型配置案例集(V5)

**Copyright © 2003-2021 新华三技术有限公司及其许可者 版权所有，保留一切权利。**

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

# 前言

本配置指导主要介绍 Comware V5 H3C 无线控制器典型配置案例集。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

## 1.1 读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

## 1.2 本书约定

### 1. 命令行格式约定






格 式	意 义
<b>粗体</b>	命令行关键字（命令中保持不变、必须照输的部分）采用 <b>加粗</b> 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x   y   ... }	表示从多个选项中仅选取一个。
[ x   y   ... ]	表示从多个选项选取一个或者不选。
{ x   y   ... } *	表示从多个选项中至少选取一个。
[ x   y   ... ] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

### 2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

### 3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

### 4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。



## 5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

## 1.3 资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: [info@h3c.com](mailto:info@h3c.com)

感谢您的反馈，让我们做得更好！

# 802.1X Auth-Fail/Guest VLAN 典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介 .....	1
2 配置前提 .....	1
3 配置举例 .....	1
3.1 组网需求 .....	1
3.2 配置思路 .....	1
3.3 配置注意事项 .....	2
3.4 配置步骤 .....	2
3.4.1 AC 的配置 .....	2
3.4.2 Switch 的配置 .....	4
3.5 验证配置 .....	5
3.6 配置文件 .....	10
4 相关资料 .....	12

# 1 简介

本文档介绍 802.1X 与 Auth-Fail VLAN、Guest VLAN 相结合的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 802.1X、SSL、WLAN 基本特性。

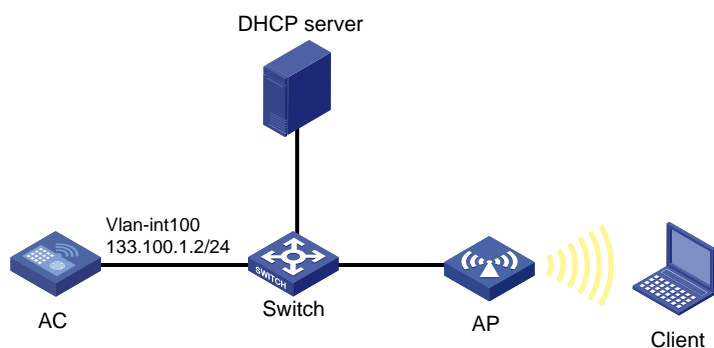
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，AC 与 AP 使用 VLAN 100 关联，Client 和 AP 被划分在不同的 VLAN 中，且 Client 和 AP 都是通过 DHCP server 获取 IP 地址。要求：

- 采用 EAP 中继方式对客户端进行本地 802.1X 认证。
- 本地 EAP 认证方法采用 peap-mschapv2。
- 当 Client 认证通过正常上线后，可以接入 VLAN 300 进行网络办公。
- 配置 Guest VLAN 400，当 Client 不进行认证时，只能进入 VLAN 400 访问特定的网络资源。
- 配置 Auth-Fail VLAN 500，当 Client 认证失败时，只能访问 VLAN 500 中的资源。

图1 802.1X 与 Auth-Fail VLAN、Guest VLAN 相结合的典型配置组网图



### 3.2 配置思路

由于本地 EAP 认证方法采用 peap-mschapv2，所以需要配置用于 EAP 认证的 SSL 服务器端策略。

## 3.3 配置注意事项

- Auth-Fail VLAN 和 Guest VLAN 都只支持 clear 类型的无线服务模板。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 133.100.1.2 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 创建 VLAN 400 作为 Guest VLAN。

```
[AC] vlan 400
[AC-vlan400] quit
```

# 创建 VLAN 500，作为 Auth-Fail VLAN。

```
[AC] vlan 500
[AC-vlan500] quit
```

# 配置 AC 的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 100、VLAN 200、VLAN 300、VLAN 400 和 VLAN 500 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300 400 500
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200、VLAN 300、VLAN 400 和 VLAN 500 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] port hybrid vlan 200 300 400 500 untagged
# 在 Hybrid 端口上使能 MAC-VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
# 在 WLAN-ESS 接口上配置端口安全模式为 802.1X 认证。
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
# 配置认证失败的用户可以访问 VLAN 500。
[AC-WLAN-ESS1] dot1x auth-fail vlan 500
# 配置未认证的用户可以访问 VLAN 400。
[AC-WLAN-ESS1] dot1x guest-vlan 400
[AC-WLAN-ESS1] quit
```

## (2) 配置无线服务

```
# 创建 clear 类型的服务模板 1。
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

## (3) 配置射频接口并绑定服务模板

```
# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN，并指定其序列号。
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行绑定。
[AC-wlan-ap-officeap-radio-2] service-template 1
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
```

## (4) 全局配置 802.1X 本地认证及用户名

```
# 全局下使能端口安全。
[AC] port-security enable
# 配置 802.1X 认证模式为 EAP。
[AC] dot1x authentication-method eap
# 创建 SSL 服务器端策略 test。
[AC] ssl server-policy test
[AC-ssl-server-policy-test] quit
# 配置 EAP Profile 为 test。
[AC] eap-profile test
# 绑定 SSL 服务器端策略 test。
```

```
[AC-eap-prof-test] ssl-server-policy test
# 配置认证方式为 peap-mschapv2。
[AC-eap-prof-test] method peap-mschapv2
[AC-eap-prof-test] quit
# 配置 local-server。
[AC] local-server authentication eap-profile test
# 配置 local-user 用户名为 user 密码为 123456。
[AC] local-user user
[AC-luser-user] password simple 123456
[AC-luser-user] service-type lan-access
[AC-luser-user] quit
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100、VLAN 200、VLAN 300、VLAN 400 和 VLAN 500，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN，VLAN 400 作为 Guest VLAN，VLAN 500 作为 Auth-Fail VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] vlan 400
[Switch-vlan400] quit
[Switch] vlan 500
[Switch-vlan500] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100~500 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300 400 500
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
```

```
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

### 3.5 验证配置

- (1) 在AC上通过 **display wlan client** 命令可以看到，当 Client 直接关联 SSID 而不进行认证时，Client 进入 VLAN 400。

```
[AC] display wlan client
```

```
Total Number of Clients      : 1
```

```
Client Information
```

```
SSID: service
```

MAC Address	User Name	APID/RID	IP Address	VLAN
0021-632f-f7bb	NULL	1 /2	0.0.0.0	400

- (2) 当 Client 使用正确的用户名和密码通过 iNode 认证上线时，Client 进入 VLAN 300。

# 在 iNode 智能客户端选择“新建”；

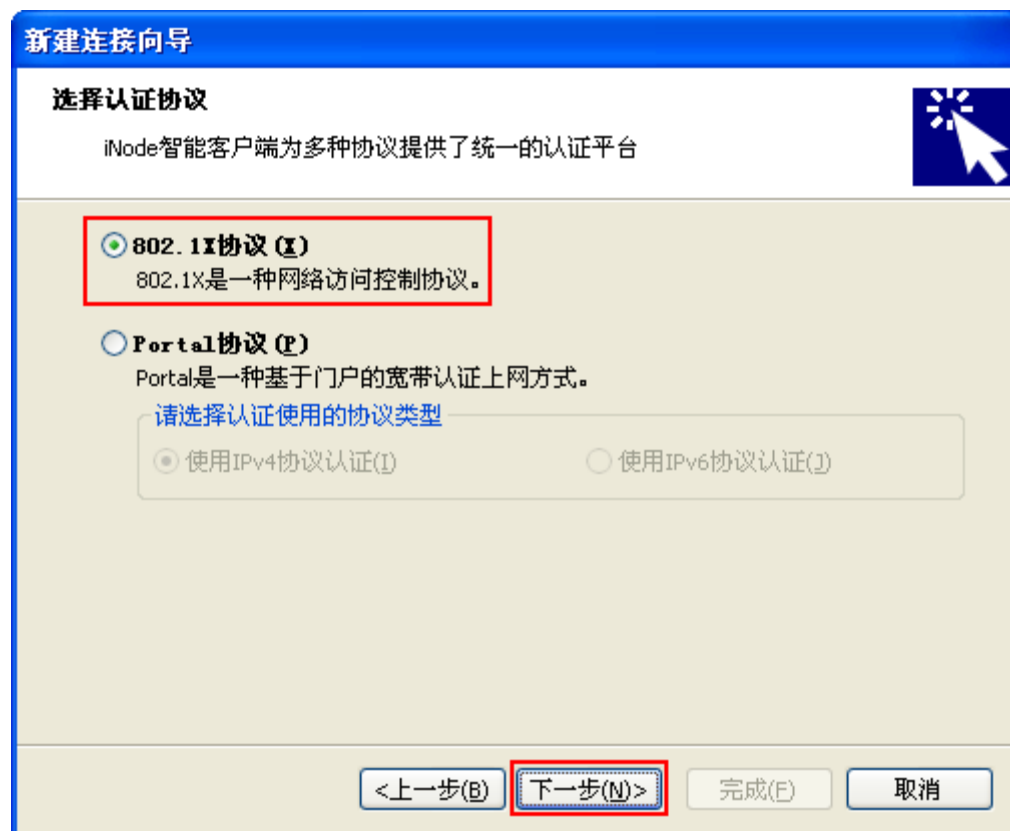


# 在弹出的“新建连接向导”中单击<下一步(N)>按钮；

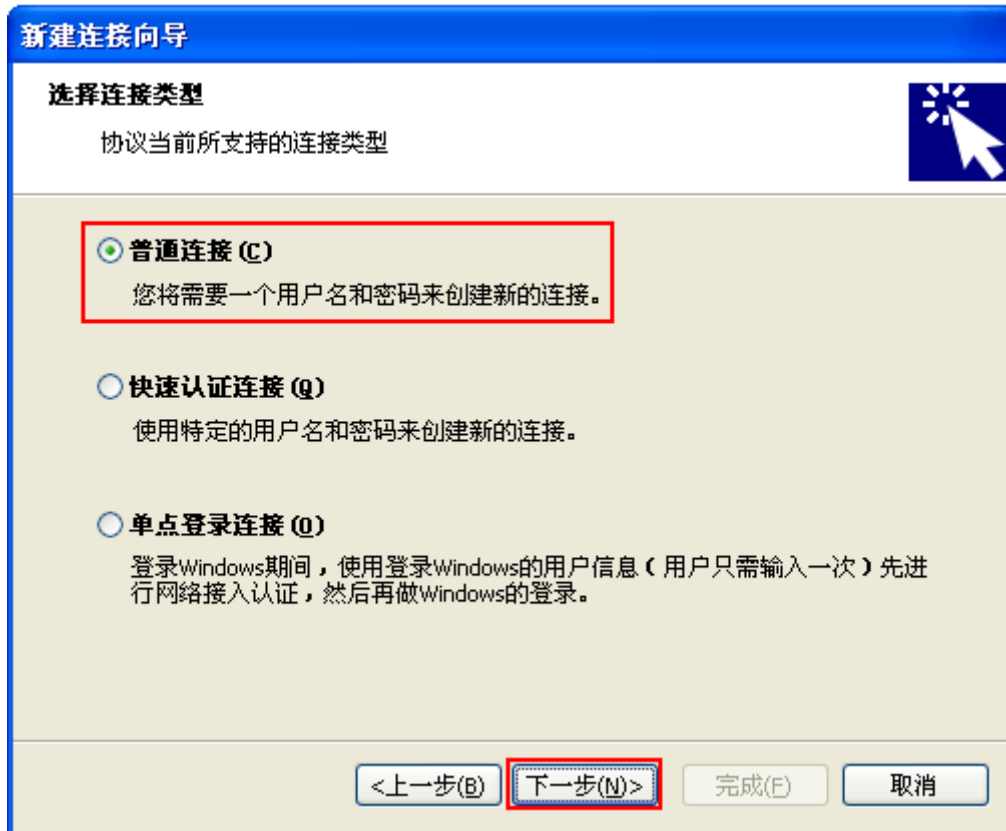




# 选择“802.1X协议(X)”，单击<下一步(N)>按钮；



# 选择“普通连接(C)”，单击<下一步(N)>按钮；



# 勾选“启用高级认证(E)”，选择“证书认证(I)”，单击<证书设置(S)...>按钮；

**新建连接向导**

**帐户信息**

您需要用户名和密码来访问网络，使用证书认证将增强通信的安全性。

连接名(C): 我的802.1X连接

用户名(U):

密码(P):

☐ 保存用户名和密码(V)

域(D):

☒ 启用高级认证(E)

☐ MAC认证(M)

☐ 智能卡认证(K)

☒ 证书认证(I)

证书设置(S)...

<上一步(B) 下一步(N)> 完成(F) 取消

# 在弹出的“证书认证高级设置”窗口中，选择认证类型为“PEAP(A)”，输入错误的用户名和密码，单击<确定>按钮；

**证书认证高级设置**

**认证类型**

☐ EAP-TLS(T)

☒ PEAP(A)

安全用户名(U): user

安全密码(W): \*\*\*\*\*

☐ 从证书读取用户名(G)

**证书选项**

选择客户端证书(S)...

☐ 验证服务器证书(V)

确定 取消

# iNode 显示信息如下：

```
认证信息
2013-07-30 19:34:41 连接网络...
2013-07-30 19:34:41 开始进行身份验证... [user]
2013-07-30 19:34:41 正在进行证书验证...
2013-07-30 19:34:43 您的身份验证成功
2013-07-30 19:34:43 自动获取IP地址...
```

# 用 **display wlan client** 命令查看设备所处 VLAN 为认证通过的 VLAN 300。

```
[AC] display wlan client
Total Number of Clients          : 1
                                Client Information
SSID: service
-----
MAC Address   User Name          APID/RID IP Address          VLAN
-----
0023-8933-21ff user              1 /2    0.0.0.0              300
-----
```

(3) 当 Client 使用错误的用户名和密码通过 iNode 认证上线时，Client 上线后进入 VLAN 500。

# 重新使用 Client 上线：

```
2013-07-30 19:37:15 开始进行身份验证... [user]
2013-07-30 19:37:15 正在进行证书验证...
2013-07-30 19:37:17 Rejected by server
2013-07-30 19:37:17 连接已断开
```

# 在 AC 上用 **display wlan client** 命令查看设备所处 VLAN 为 Auth-fail 的 VLAN 500。

```
[AC] display wlan client
Total Number of Clients          : 1
                                Client Information
SSID: service
-----
MAC Address   User Name          APID/RID IP Address          VLAN
-----
2477-0374-2cc0 user              1 /2    0.0.0.0              500
-----
```

# 在 AC 上 ping 接入的 Client，确认 Client 加入 Auth-fail 的 VLAN 并且通信正常（Client 的 IP 地址通过 DHCP 获得，可在 Client 上进行查看）。

```
[AC] ping 133.20.0.1
PING 133.20.0.1: 56 data bytes, press CTRL_C to break
```

```

Reply from 133.20.0.1: bytes=56 Sequence=0 ttl=128 time=2 ms
Reply from 133.20.0.1: bytes=56 Sequence=1 ttl=128 time=2 ms
Reply from 133.20.0.1: bytes=56 Sequence=2 ttl=128 time=1 ms
Reply from 133.20.0.1: bytes=56 Sequence=3 ttl=128 time=2 ms
Reply from 133.20.0.1: bytes=56 Sequence=4 ttl=128 time=1 ms

--- 133.20.0.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/2 ms

```

# 从下面的显示信息可以看到,MAC 地址为 0023-8933-21ff 的 Client 认证成功并进入 VLAN 300, MAC 地址为 2477-0374-2cc0 的 Client 认证失败并进入 VLAN 500 (Auth-fail VLAN), MAC 地址为 0021-632f-f7bb 的 Client 不认证则进入 VLAN 400 (Guest VLAN)。

```
[AC] display wlan client
```

```
Total Number of Clients          : 3
```

```
Client Information
```

```
SSID: service
```

MAC Address	User Name	APID/RID	IP Address	VLAN
0021-632f-f7bb	NULL	1 /2	0.0.0.0	400
0023-8933-21ff	user	1 /2	0.0.0.0	300
2477-0374-2cc0	user	1 /2	0.0.0.0	500

## 3.6 配置文件

- AC:

```

#
port-security enable
#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
vlan 500
#
local-user user
password cipher $c$3$W+cAbywSTDmIwB+87FX0qG96QjWrR9l93Q==
service-type lan-access

```

```

#
wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable
#
ssl server-policy test
#
eap-profile test
  ssl-server-policy test
  method peap-mschapv2
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200 300 400 500
#
interface Vlan-interface100
  ip address 133.100.1.2 255.255.0.0
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 300 400 500 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
  port-security port-mode userlogin-secure-ext
  dot1x guest-vlan 400
  dot1x auth-fail vlan 500
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
  service-template 1
  radio enable
#
  local-server authentication eap-profile test
#
•   Switch:
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#

```

```
vlan 500
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 100 200 300 400 500
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 100
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。

# 802.1X 热备典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

1 简介 .....	1
2 配置前提 .....	1
3 配置举例 .....	1
3.1 组网需求 .....	1
3.2 配置思路 .....	2
3.3 配置注意事项 .....	2
3.4 配置步骤 .....	2
3.4.1 AC 1 的配置 .....	2
3.4.2 AC 2 的配置 .....	6
3.4.3 Switch 的配置 .....	9
3.4.4 RADIUS server 的配置 .....	10
3.5 验证配置 .....	14
3.6 配置文件 .....	15
4 相关资料 .....	19

# 1 简介

本文档介绍无线控制器 802.1X 热备典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 802.1X 和双机热备的相关功能。

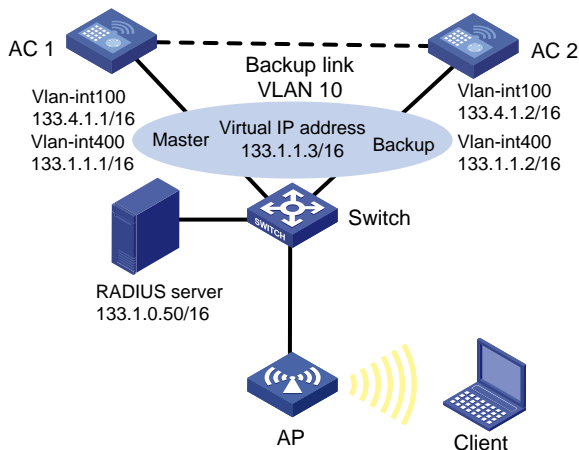
## 3 配置举例

### 3.1 组网需求

如[图1](#)所示，AC 1 和 AC 2 均支持双机热备，现要求 AC 1 和 AC 2 在运行双机热备情况下支持 802.1X 客户端的信息备份，主备 AC 切换的过程中，客户端不会重新上下线，可以继续正常通信。具体要求如下：

- 采用加密类型的服务模板，加密套件采用 AES-CCMP。
- AC 1 正常工作的情况下，Client 通过 AC 1 进行 802.1X 认证接入。AC 1 发生故障的情况下，Client 通过 AC 2 接入。
- 802.1X 的认证方式采用 EAP 中继方式。
- 采用 RADIUS 服务器作为认证服务器，RADIUS 服务器上注册的接入设备 NAS-IP 是 133.1.1.3/16。
- 防止用户通过恶意假冒其它域账号从本端口接入网络。
- 配置 VRRP 来提高链路的可靠性，保证业务流量在切换过程中不会中断。
- 将 VLAN 10 作为备份 VLAN，用于双机热备。

图1 无线控制器 802.1X 热备典型配置组网图



## 3.2 配置思路

- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此为实现 802.1X 认证，需要在 AC 上全局配置端口安全；
- 为实现 802.1X 认证状态的备份，需要配置双机热备功能；
- 在无线环境中，为了保证 AC 在切换过程中，无线服务不中断，同时使客户端的信息在 AC 间同步，需要配置双 AC 备份及 IACTP 隧道。
- 在双 AC 备份配置中，为了让 AP 优先连接到 AC 1，需要为 AC 1 配置较高的优先级。
- 在 VRRP 配置中，为了让 AC 1 成为 Master，需要为 AC 1 配置较高的优先级。
- 由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。
- 为了防止用户通过恶意假冒其它域账号从本端口接入网络，配置端口的强制认证域。

## 3.3 配置注意事项

- 主备 AC 热备相关配置必须保持一致；
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

(1) 配置 AC 1 的接口

# 创建 VLAN 10 作为双机热备的 VLAN。

```
<AC1> system-view
```

```

[AC1] vlan 10
[AC1-vlan10] quit
# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址
与 AP 建立 LWAPP 隧道。
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 133.4.1.1 16
[AC1-Vlan-interface100] quit
# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。
[AC1] vlan 200
[AC1-vlan200] quit
# 创建 VLAN 300 作为 Client 接入的业务 VLAN。
[AC1] vlan 300
[AC1-vlan300] quit
# 创建 VLAN 400 作为 RADIUS server 所在 VLAN，并配置其 IP 地址。
[AC1] vlan 400
[AC1-vlan400] quit
[AC1] interface vlan-interface 400
[AC1-Vlan-interface400] ip address 133.1.1.1 16
[AC1-Vlan-interface400] quit
# 配置 AC 1 与 Switch 连接的端口为 Trunk 模式，允许 VLAN 10、VLAN100、VLAN 200、VLAN
300、VLAN 400 通过。
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 10 100 200 300 400
[AC1-GigabitEthernet1/0/1] quit
(2) 配置无线接口
# 创建 WLAN-ESS1 接口。
[AC1] interface wlan-ess 1
# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。
[AC1-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200,禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC1-WLAN-ESS1] undo port hybrid vlan 1
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
# 开启 MAC-VLAN 功能。
[AC1-WLAN-ESS1] mac-vlan enable
[AC1-WLAN-ESS1] quit
(3) 配置无线服务
# 创建 crypto 类型的服务模板 1。
[AC1] wlan service-template 1 crypto
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC1-wlan-st-1] bind wlan-ess 1
# 设置当前服务模板的 SSID 为 service。

```

```
[AC1-wlan-st-1] ssid service
```

# 配置加密套件为 **CCMP**。

```
[AC1-wlan-st-1] cipher-suite ccmp
```

# 配置安全信息元素为 **RSN**。

```
[AC1-wlan-st-1] security-ie rsn
```

# 启用无线服务。

```
[AC1-wlan-st-1] service-template enable
```

```
[AC1-wlan-st-1] quit
```

#### (4) 配置射频接口并绑定服务模板

# 创建 **AP** 的管理模板，名称为 **officeap**，型号名称选择 **WA2620E-AGN**，并配置其序列号。

```
[AC1] wlan ap officeap model WA2620E-AGN
```

```
[AC1-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 指定该 **AP** 在 **AC 1** 上优先级为 **7**。

```
[AC1-wlan-ap-officeap] priority level 7
```

# 进入 **AP** 的 **radio 2** 视图。

```
[AC1-wlan-ap-officeap] radio 2
```

# 将服务模板 **1** 绑定到 **radio 2** 口并使能 **radio 2**。

```
[AC1-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

```
[AC1-wlan-ap-officeap-radio-2] radio enable
```

```
[AC1-wlan-ap-officeap-radio-2] return
```

#### (5) 配置 **802.1X**

# 全局开启端口安全。

```
[AC1] port-security enable
```

# 选择 **802.1X** 认证方式为 **EAP** 中继方式。

```
[AC1] dot1x authentication-method eap
```

# 进入 **WLAN-ESS1** 接口视图。

```
[AC1] interface wlan-ess 1
```

# 配置 **WLAN-ESS1** 接口的端口安全模式为 **userlogin-secure-ext**。

```
[AC1-WLAN-ESS1] port-security port-mode userlogin-secure-ext
```

# 使能 **WLAN-ESS1** 上端口安全的双机热备功能。

```
[AC1-WLAN-ESS1] port-security synchronization enable
```

# 使能 **11key** 类型的密钥协商功能。

```
[AC1-WLAN-ESS1] port-security tx-key-type 11key
```

# 指定 **802.1X** 用户使用的强制认证域 **office**，以防止恶意用户通过假冒其它域账号从本端口接入网络。

```
[AC1-WLAN-ESS1] dot1x mandatory-domain office
```

# 关闭 **802.1X** 的组播触发功能，以节省无线的通信带宽。

```
[AC1-WLAN-ESS1] undo dot1x multicast-trigger
```

# 关闭在线用户握手功能，以避免不支持在线握手功能的客户端被强制下线。

```
[AC1-WLAN-ESS1] undo dot1x handshake
```

```
[AC1-WLAN-ESS1] quit
```

#### (6) 配置 **RADIUS** 认证策略和认证域

# 创建名字为 **office** 的 **RADIUS** 方案并进入该方案视图。

```
[AC1] radius scheme office
# 配置 RADIUS 方案的主认证服务器及其通信密钥。
[AC1-radius-office] primary authentication 133.1.0.50
[AC1-radius-office] key authentication key
# 配置 AC 1 发送 RADIUS 报文使用的 nas-ip 地址为 133.1.1.3。
[AC1-radius-office] nas-ip 133.1.1.3
[AC1-radius-office] quit
# 创建 ISP 域 office，并进入其视图。
[AC1] domain office
# 为 lan-access 用户配置计费为 none，不计费。
[AC1-isp-office] accounting lan-access none
# 为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 office。
[AC1-isp-office] authentication lan-access radius-scheme office
# 为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 office。
[AC1-isp-office] authorization lan-access radius-scheme office
[AC1-isp-office] quit
```

#### (7) 配置 VRRP

```
# 在 VLAN 400 接口下创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IP 地址为 133.1.1.3。
[AC1] interface vlan-interface 400
[AC1-Vlan-interface400] vrrp vrid 1 virtual-ip 133.1.1.3
# 配置 AC 1 在备份组 1 中的优先级为 200。
[AC1-Vlan-interface400] vrrp vrid 1 priority 200
[AC1-Vlan-interface400] quit
```

#### (8) 配置双机热备

```
# 配置备份 VLAN 为 VLAN 10。
[AC1] dhrbk vlan 10
# 使能双机热备功能，且支持对称路径。
[AC1] dhrbk enable backup-type symmetric-path
# 配置双机热备模式下的设备 ID 为 1。
[AC1] nas device-id 1
```

#### (9) 配置双 AC 备份

```
# 配置备份 AC（AC 2）的 IP 地址为 133.4.1.2。
[AC1] wlan backup-ac ip 133.4.1.2
# 开启 AC 间热备份功能。
[AC1] hot-backup enable
# 配置热备 AC 间连接心跳周期为 2000 毫秒（缺省情况下，心跳周期为 2000 毫秒）。
[AC1] hot-backup hellointerval 2000
# 配置热备 AC 间数据端口的 VLAN ID 为 100。
[AC1] hot-backup vlan 100
# 配置客户端信息备份功能。
[AC1] wlan backup-client enable
```

#### (10) 配置 IACTP 隧道

```
# 配置漫游隧道，漫游组名称为 roam。
```

```
[AC1] wlan mobility-group roam
# 配置 IACTP 隧道的源地址为 133.4.1.1，成员地址为 133.4.1.2。
[AC1-wlan-mg-roam] source ip 133.4.1.1
[AC1-wlan-mg-roam] member ip 133.4.1.2
# 开启 IACTP 隧道。
[AC1-wlan-mg-roam] mobility-group enable
[AC1-wlan-mg-roam] quit
```

### 3.4.2 AC 2 的配置

#### (1) 配置 AC 2 的接口

# 创建 VLAN 10 作为双机热备的 VLAN。

```
<AC2> system-view
[AC2] vlan 10
[AC2-vlan10] quit
```

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 133.4.1.2 16
[AC2-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC2] vlan 200
[AC2-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC2] vlan 300
[AC2-vlan300] quit
```

# 创建 VLAN 400 作为 RADIUS server 所在 VLAN，并配置其 IP 地址。

```
[AC2] vlan 400
[AC2-vlan400] quit
[AC2] interface vlan-interface 400
[AC2-Vlan-interface400] ip address 133.1.1.2 16
[AC2-Vlan-interface400] quit
```

# 配置 AC 2 与 Switch 连接的端口为 Trunk 模式，允许 VLAN 10、VLAN100、VLAN 200、VLAN 300、VLAN 400 通过。

```
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 10 100 200 300 400
[AC2-GigabitEthernet1/0/1] quit
```

#### (2) 配置无线接口

# 创建 WLAN-ESS1 接口。

```
[AC2] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC2-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200,禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC2-WLAN-ESS1] undo port hybrid vlan 1
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
```

# 开启 MAC-VLAN 功能。

```
[AC2-WLAN-ESS1] mac-vlan enable
[AC2-WLAN-ESS1] quit
```

### (3) 配置无线服务

# 创建 crypto 类型的服务模板 1。

```
[AC2] wlan service-template 1 crypto
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC2-wlan-st-1] bind wlan-ess 1
```

# 设置当前服务模板的 SSID 为 service。

```
[AC2-wlan-st-1] ssid service
```

# 配置加密套件为 AES-CCMP。

```
[AC2-wlan-st-1] cipher-suite ccmp
```

# 配置安全信息元素为 RSN。

```
[AC2-wlan-st-1] security-ie rsn
```

# 启用无线服务。

```
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
```

### (4) 配置射频接口并绑定服务模板

# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN，并配置其序列号。

```
[AC2] wlan ap officeap model WA2620E-AGN
[AC2-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 AP 的 radio 2 视图。

```
[AC2-wlan-ap-officeap] radio 2
```

# 将在 AC 2 上配置的服务模板 1 与射频 2 进行关联，Client 通过服务模板 1 接入 VLAN 300。

```
[AC2-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

# 使能 AP 的 radio 2。

```
[AC2-wlan-ap-officeap-radio-2] radio enable
[AC2-wlan-ap-officeap-radio-2] return
```

### (5) 配置 802.1X

# 全局开启端口安全。

```
[AC2] port-security enable
```

# 选择 802.1X 认证方式为 EAP 中继方式。

```
[AC2] dot1x authentication-method eap
```

# 配置 WLAN-ESS1 接口的端口安全模式为 userlogin-secure-ext。

```
[AC2-WLAN-ESS1] port-security port-mode userlogin-secure-ext
```

# 使能 WLAN-ESS1 端口安全的双机热备功能。

```
[AC2-WLAN-ESS1] port-security synchronization enable
```

# 使能 11key 类型的密钥协商功能。

```
[AC2-WLAN-ESS1] port-security tx-key-type 11key
```



# 指定 802.1X 用户使用的强制认证域，以防止恶意用户通过假冒其它域账号从本端口接入网络。

```
[AC2-WLAN-ESS1] dot1x mandatory-domain office
```

# 关闭 802.1X 组播触发功能，以节省无线的通信带宽。

```
[AC2-WLAN-ESS1] undo dot1x multicast-trigger
```

# 关闭在线用户握手功能，以避免不支持在线握手功能的客户端被强制下线。

```
[AC2-WLAN-ESS1] undo dot1x handshake
```

```
[AC2-WLAN-ESS1] quit
```

## (6) 配置 RADIUS 认证策略和认证域

# 创建名字为 office 的 RADIUS 方案并进入该方案视图。

```
[AC2] radius scheme office
```

# 配置 RADIUS 方案的主认证服务器及其通信密钥。

```
[AC2-radius-office] primary authentication 133.1.0.50
```

```
[AC2-radius-office] key authentication key
```

# 配置 AC 2 发送 RADIUS 报文使用的 nas-ip 地址为 133.1.1.3。

```
[AC2-radius-office] nas-ip 133.1.1.3
```

```
[AC2-radius-office] quit
```

# 创建 ISP 域 office，并进入其视图。

```
[AC2] domain office
```

# 为 lan-access 用户配置计费为 none，不计费。

```
[AC2-isp-office] accounting lan-access none
```

# 为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 office。

```
[AC2-isp-office] authentication lan-access radius-scheme office
```

# 为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 office。

```
[AC2-isp-office] authorization lan-access radius-scheme office
```

```
[AC2-isp-office] quit
```

## (7) 配置 VRRP

# 在 VLAN 400 中配置 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 133.1.1.3。

```
[AC2] interface vlan-interface 400
```

```
[AC2-Vlan-interface400] vrrp vrid 1 virtual-ip 133.1.1.3
```

```
[AC2-Vlan-interface400] quit
```

## (8) 配置双机热备

# 配置备份 VLAN 为 VLAN 10。

```
[AC2] dhrbk vlan 10
```

# 使能双机热备功能，且支持对称路径。

```
[AC2] dhrbk enable backup-type symmetric-path
```

# 配置双机热备模式下的设备 ID 为 2。

```
[AC2] nas device-id 2
```

## (9) 配置双 AC 备份

# 配置备份 AC（AC 1）的 IP 地址为 133.4.1.1。

```
[AC2] wlan backup-ac ip 133.4.1.1
```

# 开启 AC 间热备份功能。

```
[AC2] hot-backup enable
```

# 配置热备 AC 间连接心跳周期为 2000 毫秒（缺省情况下，心跳周期为 2000 毫秒）。

```

[AC2] hot-backup hellointerval 2000
# 配置热备 AC 间数据端口的 VLAN ID 为 100。
[AC2] hot-backup vlan 100
# 配置客户端信息备份功能。
[AC2] wlan backup-client enable
(10) 配置 IACTP 隧道
# 配置漫游隧道，漫游组名称为 roam。
[AC2] wlan mobility-group roam
# 配置 IACTP 隧道的源地址为 133.4.1.2，成员地址为 133.4.1.1。
[AC2-wlan-mg-roam] source ip 133.4.1.2
[AC2-wlan-mg-roam] member ip 133.4.1.1
# 开启 IACTP 隧道。
[AC2-wlan-mg-roam] mobility-group enable
[AC2-wlan-mg-roam] quit

```

### 3.4.3 Switch 的配置

# 创建 VLAN 100、VLAN 300 和 VLAN 400，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN，VLAN 400 作为 RADIUS server 所在 VLAN。

```

<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] vlan 400
[Switch-vlan400] quit
# 配置 Switch 与 AC 1 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 10、VLAN 100~400 通过。
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 10 100 200 300 400
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AC 2 相连的 GigabitEthernet1/0/2 接口的属性为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 10、VLAN 100~400 通过。
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 10 100 200 300 400
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 RADIUS server 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 400 通过。

```

```
[Switch] interface GigabitEthernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 400
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/4 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
```

### 3.4.4 RADIUS server 的配置



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)），说明 RADIUS 服务器的基本配置。

---

# 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，单击<增加>按钮，进入“增加接入设备”页面，单击<手工增加>按钮，进入“手工增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“key”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 133.1.1.3 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

接入配置

认证端口 \*

1812

计费端口 \*

1813

组网方式

不启用混合组网

业务类型

LAN接入业务

接入设备类型

H3C(General)

接入设备分组

无

共享密钥 \*

...

确认共享密钥 \*

...

业务分组

未分组

设备列表

选择

手工增加

设备名称

未找到符合条件的记录。

共有0条记录。

手工增加接入设备

起始IP地址 \*

133.1.1.3

结束IP地址

备注

确定

取消

备注

删除

- # 配置接入策略。
- 选择“用户”页签，单击导航树中的[用户/接入策略管理/接入策略管理]菜单项，单击<增加>按钮，创建一条接入策略。
- 接入策略名输入“802.1x”。
  - 证书认证选择“EAP 证书认证”。
  - 证书认证类型选择“EAP-PEAP 认证”。
  - 认证证书子类型选择“MS-CHAPV2 认证”。
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 配置接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 \*

802.1x

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☐ 不启用

☒ EAP证书认证

☐ WAP证书认证

认证证书类型

EAP-PEAP认证

认证证书子类型

MS-CHAPV2认证

下发VLAN

下发用户组

☐ 下发User Profile

☐ 下发ACL

- # 增加接入服务配置。
- 选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，单击<增加>按钮，创建一条接入服务。
- 服务名输入“802.1x”。

- 缺省接入策略选择之前创建的策略“802.1x”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 配置接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 \*

802.1x

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

802.1x

缺省安全策略 \*

不使用

缺省内网外联配置 \*

不使用

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 (PC

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

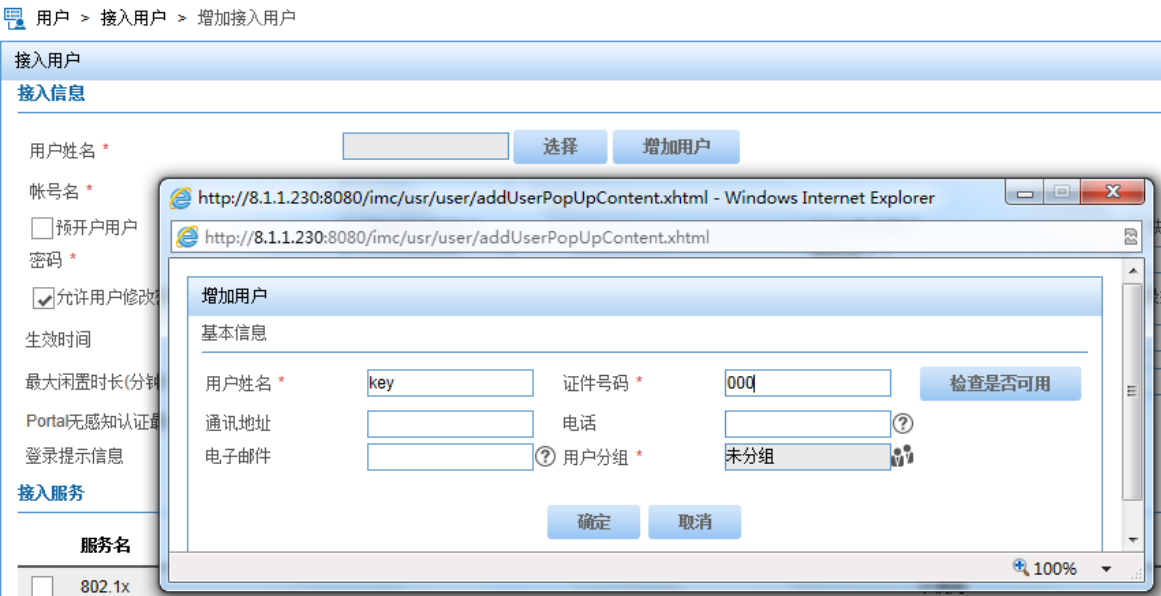
名称	接入策略	安全策略	私有属性下发策略	内网外联配置	BYOD页面
未找到符合条件的记录。					

确定

取消

- # 增加用户配置。
- 选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，单击<增加>按钮，增加一个接入用户。
- 单击“增加用户”。
  - 用户姓名输入“key”。
  - 证件号码输入“000”。
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 增加用户配置



# 增加接入用户配置。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，单击<增加>按钮，增加一个接入用户。

- 单击“选择”按钮，在页面中选择上面创建的用户“key”。
- 账号名输入“key”。
- 密码与密码确认输入“123456”。
- 选择服务名“802.1x”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加接入用户配置



## 3.5 验证配置

- (1) Client 进行 802.1X 认证上线, 输入用户名 “key” 和密码 “123456” 后, 认证成功。
- (2) 在 AC 1 上使用 **display wlan client** 命令查看 Client 的上线 VLAN 信息, 可以看到 Client 使用 VLAN 300 上线。

```
[AC1] display wlan client
Total Number of Clients          : 1
                                Client Information
SSID: service
-----
MAC Address   User Name          APID/RID IP Address          VLAN
-----
0022-3f90-938e key              1 /2    0.0.0.0              300
-----
```

- (3) 使用 **display connection** 命令查看连接信息, 可以看到只有一个客户端与 AC 1 建立了连接。

```
[AC1] display connection

Index=5 ,Username=key@office
MAC=00-22-3F-90-93-8E
IP=N/A
IPv6=N/A
Total 1 connection(s) matched.
```

- (4) 在 AC 2 上使用 **display wlan client** 命令查看 Client 的上线 VLAN 信息, 同样可以看到 Client 使用 VLAN 300 上线。此处 AP 为 Backup 状态, 实际是 AC 1 备份过来的 Client。

```
<AC2> display wlan client
Total Number of Clients          : 1
                                Client Information
SSID: service
-----
MAC Address   User Name          APID/RID IP Address          VLAN
-----
0022-3f90-938e key              1 /2    0.0.0.0              300
-----
```

- (5) 使用 **display connection** 命令查看连接信息, 可以看到只有一个客户端与 AC 2 建立了连接。

```
<AC2> display connection

Index=4 ,Username=key@office
MAC=00-22-3F-90-93-8E
IP=N/A
IPv6=N/A
Total 1 connection(s) matched.
```

- (6) 将 AC 1 断开, 可以发现 Client 未下线, 仍然可以正常通信。

## 3.6 配置文件

- AC 1:

```
#
nas device-id 1
#
port-security enable
#
dot1x authentication-method eap
#
wlan backup-ac ip 133.4.1.2
#
hot-backup enable domain 1
hot-backup vlan 100
#
wlan backup-client enable
#
vlan 10
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
radius scheme office
primary authentication 133.1.0.50
key authentication cipher $c$3$HkosOaXlBAk6R6vIM+mukgyhrgxTw==
nas-ip 133.1.1.3
#
domain office
authentication lan-access radius-scheme office
authorization lan-access radius-scheme office
accounting lan-access none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 1
cipher-suite ccmp
security-ie rsn
service-template enable
#
```



```

interface Vlan-interface100
 ip address 133.4.1.1 255.255.0.0
#
interface Vlan-interface400
 ip address 133.1.1.1 255.255.0.0
 vrrp vrid 1 virtual-ip 133.1.1.3
 vrrp vrid 1 priority 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 10 200 300 400
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
 port-security synchronization enable
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type llkey
 undo dot1x handshake
 dot1x mandatory-domain office
 undo dot1x multicast-trigger
#
wlan ap officeap model WA2620E-AGN id 1
 priority level 7
 serial-id 21023529G007C000020
 radio 1
 radio 2
 service-template 1 vlan-id 300
 radio enable
#
wlan mobility-group roam
 member ip 133.4.1.2
 source ip 133.4.1.1
 mobility-group enable
#
dhbk enable backup-type symmetric-path
dhbk vlan 10
#
● AC 2:
#
nas device-id 2
#
port-security enable
#
dot1x authentication-method eap

```

```

#
wlan backup-ac ip 133.4.1.1
#
hot-backup enable domain 1
hot-backup vlan 100
#
wlan backup-client enable
#
vlan 10
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
radius scheme office
primary authentication 133.1.0.50
key authentication cipher $c$3$nHkosOaXlBAk6R6vIM+mukgyhrgxTw==
nas-ip 133.1.1.3
#
domain office
authentication lan-access radius-scheme office
authorization lan-access none
accounting lan-access none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 1
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface Vlan-interface100
ip address 133.4.1.2 255.255.0.0
#
interface Vlan-interface400
ip address 133.1.1.2 255.255.0.0
vrrp vrid 1 virtual-ip 133.1.1.3
#
interface GigabitEthernet1/0/1
port link-type trunk

```

```

port trunk permit vlan 10 200 300 400
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
port-security synchronization enable
port-security port-mode userlogin-secure-ext
port-security tx-key-type llkey
undo dot1x handshake
dot1x mandatory-domain office
undo dot1x multicast-trigger
#
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1 vlan-id 300
radio enable
#
wlan mobility-group roam
member ip 133.4.1.1
source ip 133.4.1.2
mobility-group enable
#
dhbk enable backup-type symmetric-path
dhbk vlan 10
#
● Switch:
#
vlan 10
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 10 100 200 300 400
port trunk pvid vlan 100
#

```

```
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 10 100 200 300 400
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 400
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 802.1X 认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介 .....	1
2 配置前提 .....	1
3 配置举例 .....	1
3.1 组网需求 .....	1
3.2 配置思路 .....	1
3.3 配置注意事项 .....	1
3.4 配置步骤 .....	2
3.4.1 AC 的配置 .....	2
3.4.2 RADIUS 服务器的配置 .....	4
3.5 验证配置 .....	6
3.6 配置文件 .....	9
4 相关资料 .....	11

# 1 简介

本文档介绍无线控制器 802.1X 认证典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、802.1X、WLAN 特性。

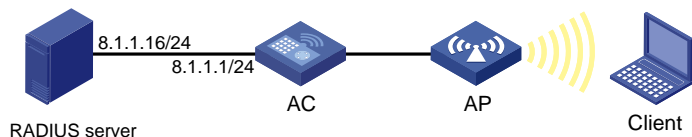
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示组网，采用 iMC 作为 RADIUS 服务器，要求：

- 在 AC 上启用 802.1X 远程认证，实现对 Client 的接入控制。
- 802.1X 认证方式采用 EAP 中继方式。
- 采用加密类型的服务模板，加密套件采用 TKIP。

图1 802.1X 远程认证组网图



### 3.2 配置思路

- 由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。

### 3.3 配置注意事项

- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) AC 接口的配置

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 8.1.1.1 255.255.255.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200，作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

#### (2) 配置接口 WLAN-ESS 1

# 创建 WLAN-ESS1 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 开启 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

#### (3) 配置无线服务

# 创建 crypto 类型的服务模板 1。

```
[AC] wlan service-template 1 crypto
```

# 配置当前服务模板的 SSID 为 joe\_dot1x。

```
[AC-wlan-st-1] ssid joe_dot1x
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind WLAN-ESS 1
```

# 配置加密套件为 TKIP。

```
[AC-wlan-st-1] cipher-suite tkip
```

# 配置在 AP 发送信标和探查响应帧时携带 WPA IE 信息。

```
[AC-wlan-st-1] security-ie wpa
```

# 使能服务模板。

```
[AC-wlan-st-1] service-template enable
```



```
[AC-wlan-st-1] quit
```

#### (4) 配置 AP 并绑定无线服务

# 创建 AP 模板，名称为 officeap1，型号名称选择 WA2620E-AGN，该 AP 的序列号为 21023529G007C000020。

```
[AC] wlan ap officeap1 model WA2620E-AGN
```

```
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
```

# 进入 AP 的 radio 2 视图。

```
[AC-wlan-ap-officeap1] radio 2
```

# 将服务模板 1 绑定到 radio 2 口并使能 radio 2。

```
[AC-wlan-ap-officeap1-radio-2] service-template 1
```

```
[AC-wlan-ap-officeap1-radio-2] radio enable
```

```
[AC-wlan-ap-officeap1-radio-2] quit
```

#### (5) 配置 RADIUS 方案

# 创建 RADIUS 方案 rad。

```
[AC] radius scheme rad
```

# 配置主认证 RADIUS 服务器的 IP 地址 8.1.1.16。

```
[AC-radius-rad] primary authentication 8.1.1.16
```

# 配置主计费 RADIUS 服务器的 IP 地址 8.1.1.16。

```
[AC-radius-rad] primary accounting 8.1.1.16
```

# 配置与认证 RADIUS 服务器交互报文时的共享密钥为 expert。

```
[AC-radius-rad] key authentication expert
```

# 配置与计费 RADIUS 服务器交互报文时的共享密钥为 expert。

```
[AC-radius-rad] key accounting expert
```

# 配置 RADIUS 服务器的服务类型为 extended。

```
[AC-radius-rad] server-type extended
```

```
[AC-radius-rad] quit
```

#### (6) 配置 domain 域

# 创建 ISP 域 imc。

```
[AC] domain imc
```

# 为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 rad。

```
[AC-isp-imc] authentication lan-access radius-scheme rad
```

# 为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 rad。

```
[AC-isp-imc] authorization lan-access radius-scheme rad
```

# 为 lan-access 用户配置计费方案为 RADIUS 方案，方案名为 rad。

```
[AC-isp-imc] accounting lan-access radius-scheme rad
```

```
[AC-isp-imc] quit
```

# 配置缺省的 ISP 域为 imc。

```
[AC] domain default enable imc
```

#### (7) 配置 802.1X

# 使能端口安全。

```
[AC] port-security enable
```

# 配置 802.1X 用户的认证方式为 EAP 中继方式。

```
[AC] dot1x authentication-method eap
```

# 进入 WLAN-ESS1 接口视图。  
[AC] interface wlan-ess 1  
# 配置端口的安全模式为 userLogin-SecureExt。  
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext  
# 在接口 WLAN-ESS1 下使能 11key 类型的密钥协商功能。  
[AC-WLAN-ESS1] port-security tx-key-type 11key  
# 关闭 802.1X 组播触发功能和在线用户握手功能。  
[AC-WLAN-ESS1] undo dot1x multicast-trigger  
[AC-WLAN-ESS1] undo dot1x handshake  
[AC-WLAN-ESS1] quit

3.4.2 RADIUS 服务器的配置



下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.2(E0401)、iMC UAM 5.2(E0402)），说明 RADIUS 服务器的基本配置。

- # 增加接入设备。
- 登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[用户接入管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。
- 设置与 AC 交互报文时使用的认证、计费共享密钥为“expert”；
  - 设置认证及计费的端口号分别为“1812”和“1813”；
  - 选择业务类型为“LAN 接入业务”；
  - 选择接入设备类型为“H3C”；
  - 选择或手工增加接入设备，添加 IP 地址为 8.1.1.1 的接入设备；
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

业务 >> 用户接入管理 >> 接入设备管理 >> 接入设备配置 >> 增加接入设备

接入配置

\* 认证端口

1812

\* 共享密钥

\*\*\*\*\*

接入区域

无

接入设备类型

H3C(General)

业务分组

未分组

\* 计费端口

1813

\* 确认共享密钥

\*\*\*\*\*

业务类型

LAN接入业务

组网方式

不启用混合组网

设备列表

选择

手工增加

全部清除

共有1条记录。

设备名称	设备IP地址	设备型号	备注	删除
	8.1.1.1			✖

确定

取消

# 增加服务配置。

选择“业务”页签，单击导航树中的[用户接入管理/服务配置管理]菜单项，进入服务列表页面，在该页面中单击“增加”按钮，进入增加服务配置页面。

- 输入服务名“dot1x auth”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 增加服务配置

业务 >> 用户接入管理 >> 服务配置管理 >> 增加服务配置

帮助

基本信息

服务名

dot1x auth

业务分组

未分组

缺省安全策略

不使用安全策略

缺省私有属性下发策略

不使用

计费策略

不计费

服务描述

☒ 可申请

☐ Portal智能终端快速认证

服务后缀

缺省接入规则

禁止接入

缺省内网外联配置

不使用

接入策略列表

增加

接入场景

接入规则

安全策略

私有属性下发策略

内网外联配置

优先级

修改

删除

确定

取消

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 输入用户姓名；
- 输入账号名“localuser”和密码；
- 在接入服务处选择“dot1x auth”；
- 单击<确定>按钮完成操作。

图4 增加接入用户

用户 >> 所有接入用户 >> 增加接入用户

帮助

接入用户

接入信息

用户姓名

test

选择

增加用户

帐号名

localuser

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码

\*\*\*\*\*

密码确认

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

失效日期

最大闲置时长

分钟

帐号类型

预付费

自动充值

允许

登录提示信息

Portal智能终端最大绑定数

1

在线数量限制

1

预付金额

0

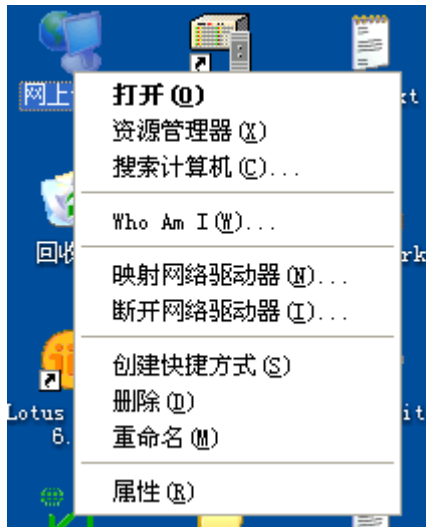
元

接入服务

服务名	服务后缀	缺省安全策略	状态	计费策略	分配IP地址
<input checked="" type="checkbox"/> dot1x auth	aabcc.net	不使用安全策略	可申请	UserAcct	

### 3.5 验证配置

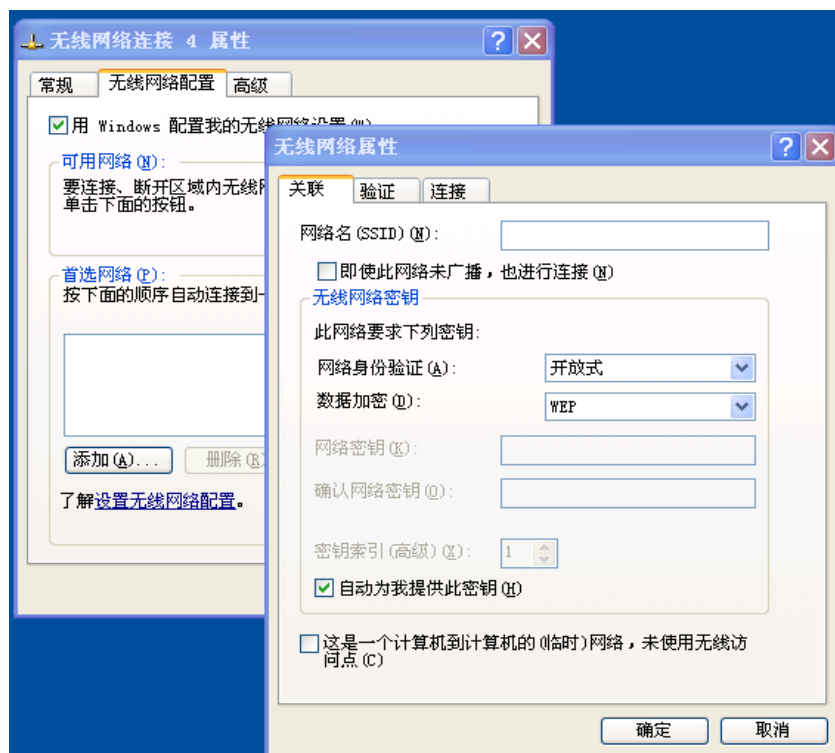
# 本文以 XP 系统为例，右键点击桌面上网络邻居，点击“属性”。



# 弹出网络连接窗口后，右键点击“无线网络连接”图标，选择“属性”。

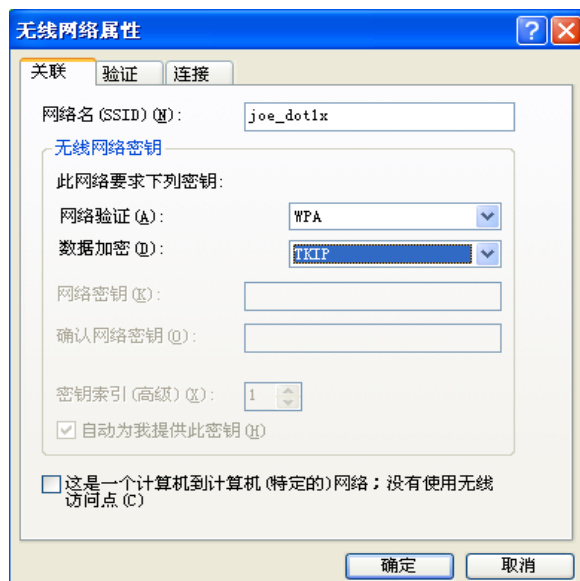


# 在弹出的对话框中，点击“无线网络配置”页签，点击<添加>按钮。

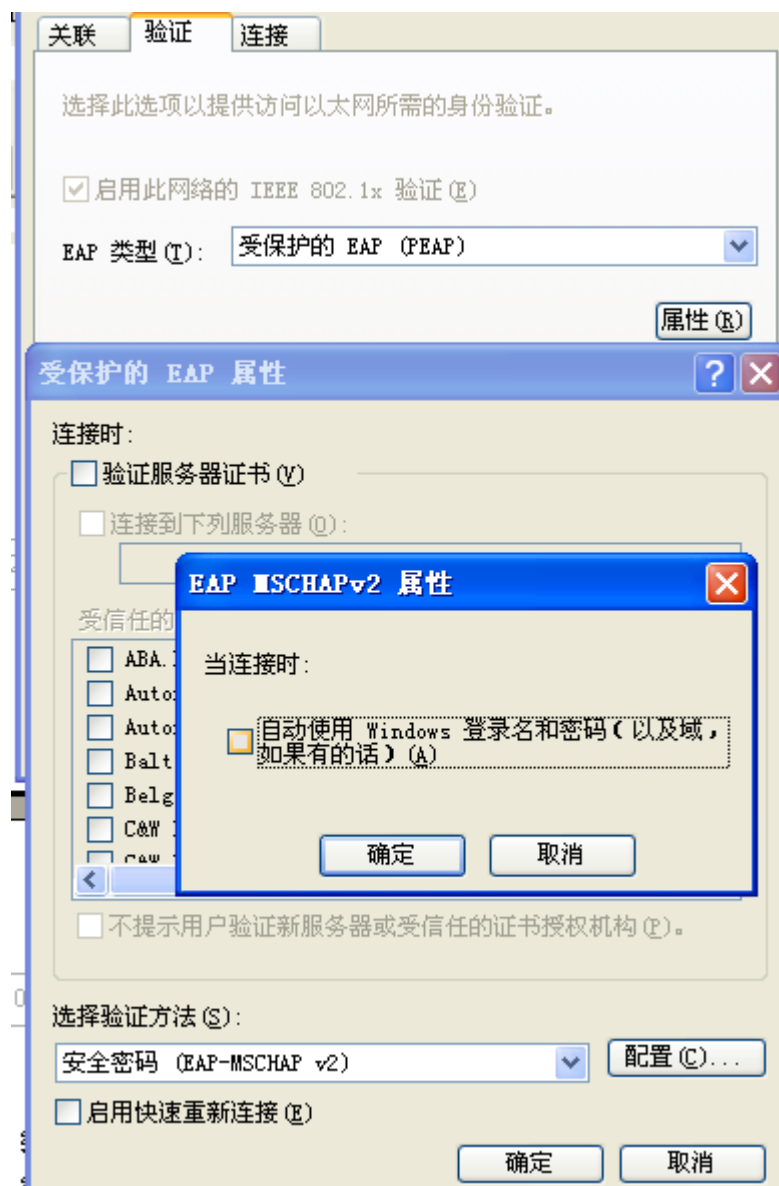


# 在弹出的“无线网络属性”对话框中，添加 SSID，并选择相应的加密方式、认证方式。

- 在网络名添加“joe\_dot1x”的 SSID。
- 在无线网络密钥处，选择网络验证 WPA。
- 在数据加密处，选择加密类型为 TKIP。



- 点击“验证”页签，在 EAP 类型处，选择“受保护的 EAP (PEAP)”。
- 点击<属性>按钮，在弹出的对话框中取消“验证服务器证书”，选择验证方法为“安全密码 (EAP-MSCHAP v2)”。
- 点击<配置>按钮，取消“自动使用 Windows 登录名和密码 (以及域，如果有的话)”。



# 当用户通过认证连接到 AP 后，可以在 AC 上使用 **display connection** 查看有 1 个用户在线。

```
<AC> display connection
Index=5 ,Username=test@imc
MAC=00-19-5B-EC-7A-E9
IP=N/A
IPv6=N/A
Total 1 connection(s) matched.
```

# 在 AC 上使用 **display connection ucibindex** 查看用户的较详细信息。

```
<AC> display connection ucibindex 5
Index=5 , Username=test@imc
MAC=00-19-5B-EC-7A-E9
IP=N/A
IPv6=N/A
Access=8021X ,AuthMethod=EAP
```

```
Port Type=Wireless-802.11,Port Name=WLAN-DBSS0:2
Initial VLAN=1, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2014-1-14 15:24:21 ,Current=2014-1-14 18:29:24 ,Online=03h05m03s
Total 1 connection matched.
```

# 在 AC 上使用 **display wlan client verbose** 查看终端信息。

```
<AC> display wlan client verbose
Total Number of Clients : 1
Client Information
-----
MAC Address : 0019-5bec-7ae9
User Name : test
AID : 1
AP Name : officeap1
Radio Id : 2
SSID : joe_dot1x
BSSID : 0023-8998-0450
Port : WLAN-DBSS0:2
VLAN : 100
State : Running
Power Save Mode : Active
Wireless Mode : 11g
QoS Mode : WMM
Listen Interval (Beacon Interval) : 10
RSSI : 32
Rx/Tx Rate : 54/54
Client Type : WPA
Authentication Method : Open System
AKM Method : Dot1X
4-Way Handshake State : PTKINITDONE
Group Key State : IDLE
Encryption Cipher : TKIP
Roam Status : Normal
Roam Count : 0
Up Time (hh:mm:ss) : 00:54:47
```

## 3.6 配置文件

```
#
domain default enable imc
#
port-security enable
#
dot1x authentication-method eap
#
```

```

vlan 100
#
vlan 200
#
radius scheme rad
    server-type extended
    primary authentication 8.1.1.16
    primary accounting 8.1.1.16
    key authentication cipher $c$3$21zk+lCairQXsBSeu53rIVaO77HxHzOMXQ==
    key accounting cipher $c$3$kQDj+ARtECao65pwIoPggsaj34Vxmbj7sA==
#
domain imc
    authentication lan-access radius-scheme rad
    authorization lan-access radius-scheme rad
    accounting lan-access radius-scheme rad
    access-limit disable
    state active
    idle-cut disable
    self-service-url disable
#
wlan service-template 1 crypto
    ssid joe_dot1x
    bind WLAN-ESS 1
    cipher-suite tkip
    security-ie wpa
    service-template enable
#
interface Vlan-interface100
    ip address 8.1.1.1 255.255.255.0
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
    port-security port-mode userlogin-secure-ext
    port-security tx-key-type 11key
    undo dot1x handshake
    undo dot1x multicast-trigger
#
wlan ap officeap1 model WA2620E-AGN id 1
    serial-id 21023529G007C000020
    radio 1
    radio 2
        service-template 1
        radio enable
#

```



## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 802.1X 与 LDAP 组合认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提 .....	1
3 配置举例 .....	1
3.1 组网需求 .....	1
3.2 配置思路 .....	2
3.3 配置注意事项.....	2
3.4 配置步骤 .....	2
3.5 验证配置 .....	5
3.6 配置文件 .....	6
4 相关资料 .....	8

# 1 简介

本文档介绍在无线控制器上配置本地 802.1X 认证，通过 LDAP 协议将 AC 设备解析出的用户名和密码传到 LDAP 服务器上对无线用户进行认证的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA 和 802.1X 特性。

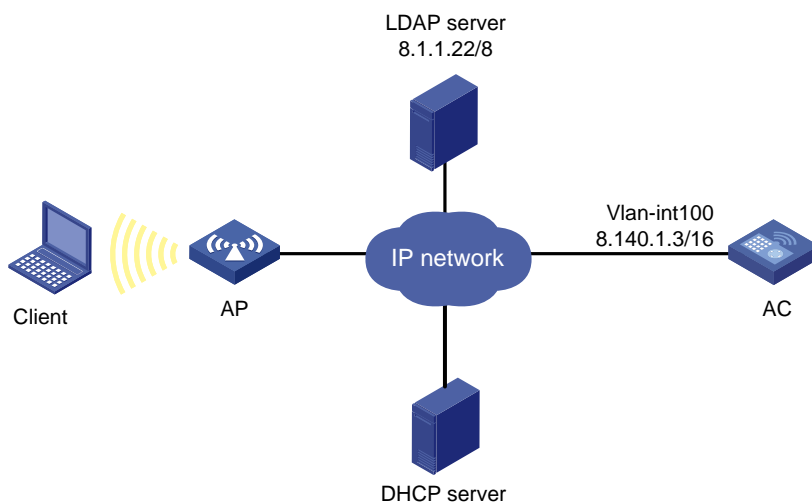
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，Client 和 AP 通过 DHCP 服务器获得 IP 地址，要求：

- 在 AC 上配置 EAP 中继方式的 802.1X 认证，以控制 Client 对网络资源的访问。
- 通过 LDAP 服务器对 Client 进行身份信息的存储和验证。
- 配置 WLAN-ESS 接口使能密钥协商功能。
- 对 AC 和 Client 之间的数据传输进行加密，加密套件采用 AES-CCMP。
- EAP 认证方式采用 TLS 和 PEAP-GTC，优先使用 TLS。

图1 802.1X 与 LDAP 组合认证组网图



## 3.2 配置思路

- 由于网络中部署了 LDAP 服务器对 Client 进行身份认证，因此需要在 AC 上配置本地 EAP 服务器来协助完成 EAP 认证。
- 为了优先使用 TLS 的 EAP 认证方式，在配置顺序上必须先配置 TLS 认证方式，后配置 PEAP-GTC 的认证方式。
- 由于 EAP 认证方式采用 TLS 和 PEAP-GTC，所以必须配置 SSL 服务器端策略。
- 由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。
- 为了防止用户通过恶意假冒其它域账号从本端口接入网络，配置端口的强制认证域。

## 3.3 配置注意事项

- 当端口安全功能处于使能状态时，端口上的 802.1X 功能将不能被手动开启，且 802.1X 端口接入控制方式和端口接入控制模式也不能被修改，只能随端口安全模式的改变由系统更改。
- 在端口上有用户在线的情况下，端口安全功能无法关闭。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

## 3.4 配置步骤

### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface1] ip address 8.140.1.3 255.255.0.0
[AC-Vlan-interface1] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

### (2) 配置无线接口

# 创建 WLAN-ESS0 接口，并进入该视图。

```
[AC] interface wlan-ess 0
# 配置端口的链路类型为 Hybrid。
[AC-WLAN-ESS0] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS0] port hybrid pvid vlan 200
[AC-WLAN-ESS0] port hybrid vlan 200 untagged
# 在 Hybrid 端口上使能 MAC-VLAN 功能。
[AC-WLAN-ESS0] mac-vlan enable
[AC-WLAN-ESS0] quit
```

### (3) 配置无线服务

```
# 创建 crypto 类型的服务模板 1。
[AC] wlan service-template 1 crypto
# 配置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS0 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 0
# 使能 AES-CCMP 加密套件。
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
# 使能无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### (4) 配置 AP 并绑定无线服务

```
# 在 AC 上配置 AP 名称为 ap1，型号名称 WA2620E-AGN，并配置 AP 的序列号。
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 21023529G007C000020
# 进入射频 2 视图。
[AC-wlan-ap-ap1] radio 2
# 将无线服务 1 绑定到射频 2。
[AC-wlan-ap-ap1-radio-2] service-template 1
# 使能 AP 的 radio 2。
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

### (5) 配置 LDAP 认证

```
# 创建 LDAP 方案 ldap1 并进入其视图。
[AC] ldap scheme ldap1
# 配置 LDAP 服务器的 IP 地址 8.1.1.22。
[AC-ldap-ldap1] authentication-server 8.1.1.22
# 配置具有管理员权限的用户 DN。
[AC-ldap-ldap1] login-dn cn=administrator,cn=users,dc=myias,dc=com
# 配置具有管理员权限的用户密码。
[AC-ldap-ldap1] login-password simple admin!123456
```

# 配置查询用户的起始目录。

```
[AC-ldap-ldap1] user-parameters search-base-dn dc=myias,dc=com
```

```
[AC-ldap-ldap1] quit
```

## (6) 配置 802.1X 认证

# 启用端口安全。

```
[AC] port-security enable
```

# 配置 802.1X 认证方式为 EAP 中继方式。

```
[AC] dot1x authentication-method eap
```

# 创建 office 域并进入其视图。

```
[AC] domain ldap
```

# 为 lan-access 用户配置认证方法为本地认证。

```
[AC-isp-ldap] authentication lan-access local
```

# 为 lan-access 用户配置授权方法为不授权

```
[AC-isp-ldap] authorization lan-access none
```

# 为 lan-access 用户配置计费为 none，不计费。

```
[AC-isp-ldap] accounting lan-access none
```

```
[AC-isp-ldap] quit
```

# 进入 WLAN-ESS 接口视图。

```
[AC] interface wlan-ess 0
```

# 配置端口的安全模式为 userLogin-SecureExt。

```
[AC-WLAN-ESS0] port-security port-mode userlogin-secure-ext
```

# 在接口 WLAN-ESS0 下使能 11key 类型的密钥协商功能。

```
[AC-WLAN-ESS0] port-security tx-key-type 11key
```

# 关闭在线用户握手功能。

```
[AC-WLAN-ESS0] undo dot1x handshake
```

# 关闭 802.1X 的组播触发功能。

```
[AC-WLAN-ESS0] undo dot1x multicast-trigger
```

# 指定 ESS 口的认证域为 ldap。

```
[AC-WLAN-ESS0] dot1x mandatory-domain ldap
```

```
[AC-WLAN-ESS0] quit
```

## (7) 配置 SSL 服务器端策略

# 创建 PKI 实体 en，通用名 common。

```
[AC] pki entity en
```

```
[AC-pki-entity-en] common-name common
```

```
[AC-pki-entity-en] quit
```

# 创建 PKI 域 do，本端实体 en，注册机构：CA，不启用 CRL 查询。

```
[AC] pki domain do
```

```
[AC-pki-domain-do] certificate request from ca
```

```
[AC-pki-domain-do] certificate request entity en
```

```
[AC-pki-domain-do] crl check disable
```

```
[AC-pki-domain-do] quit
```

# 先用 FTP 等方式把证书上传到无线控制器中，再用命令导入证书。

```
[AC] pki import-certificate ca domain do pem filename root.pem
```

```
[AC] pki import-certificate local domain do p12 filename server.pfx
```

# 配置 SSL 服务器端策略 **eap-policy**，指定使用的 PKI 域为 **do**。

```
[AC] ssl server-policy eap-policy
[AC-ssl-server-policy-eap-policy] pki-domain do
[AC-ssl-server-policy-eap-policy] quit
```

(8) 配置本地 EAP 认证

# 配置 EAP Profile，指定认证方法为 EAP-TLS 和 PEAP-GTC。

```
[AC] eap-profile default-profile
[AC-eap-prof-default-profile] ssl-server-policy eap-policy
[AC-eap-prof-default-profile] method tls
[AC-eap-prof-default-profile] method peap-gtc
```

# 配置使用 LDAP 数据库查询用户身份，引用 LDAP 方案 **ldap1**。

```
[AC-eap-prof-default-profile] user-credentials ldap-scheme ldap1
[AC-eap-prof-default-profile] quit
```

# 配置本地服务器认证所使用的 **eap-profile** 为 **default-profile**。

```
[AC] local-server authentication eap-profile default-profile
```

# 配置无线控制器去往 LDAP 服务器的静态路由。

```
[AC] ip route-static 8.0.0.0 255.0.0.0 8.140.1.1
```

## 3.5 验证配置

# 当用户通过认证连接到 AC 后，可以在 AC 上使用 **display connection** 查看有 1 个用户在线。

```
<AC> display connection
  Index=5 ,Username=client@ldap
MAC=00-19-5B-EC-7A-E9
IP=N/A
IPv6=N/A
Total 1 connection(s) matched.
```

# 在 AC 上使用 **display connection ucibindex** 查看用户的较详细信息。

```
<AC> display connection ucibindex 5
Index=5 , Username=client@ldap
MAC=00-19-5B-EC-7A-E9
IP=N/A
IPv6=N/A
Access=8021X ,AuthMethod=EAP
Port Type=Wireless-802.11,Port Name=WLAN-DBSS0:2
Initial VLAN=300, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2014-1-14 15:24:21 ,Current=2014-1-14 18:29:24 ,Online=03h05m03s
Total 1 connection matched.
```

# 在 AC 上使用 **display wlan client verbose** 查看终端信息。

```
<AC> display wlan client verbose
Total Number of Clients : 1
Client Information
```



```
-----  
MAC Address : 0019-5bec-7ae9  
User Name : client  
AID : 1  
AP Name : ap1  
Radio Id : 2  
SSID : service  
BSSID : 0023-8998-0450  
Port : WLAN-DBSS0:2  
VLAN : 300  
State : Running  
Power Save Mode : Active  
Wireless Mode : 11g  
QoS Mode : WMM  
Listen Interval (Beacon Interval) : 10  
RSSI : 32  
Rx/Tx Rate : 54/54  
Client Type : WPA2(RSN)  
Authentication Method : Open System  
AKM Method : Dot1X  
4-Way Handshake State : PTKINITDONE  
Group Key State : IDLE  
Encryption Cipher : AES-CCMP  
Roam Status : Normal  
Roam Count : 0  
Up Time (hh:mm:ss) : 00:54:47
```

## 3.6 配置文件

```
#  
port-security enable  
#  
dot1x authentication-method eap  
#  
vlan 100  
#  
vlan 200  
#  
vlan 300  
#  
ldap scheme ldap1  
authentication-server 8.1.1.22  
login-dn cn=administrator,cn=users,dc=myias,dc=com  
login-password cipher $c$3$5emHSGcXd0kZPDCjh5zpTV+vrAR3aNUd  
user-parameters search-base-dn dc=myias,dc=com  
#  
domain ldap  
authentication lan-access local
```

```

authorization lan-access none
accounting lan-access none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
pki entity en
    common-name common
#
pki domain do
    certificate request from ca
    certificate request entity en
    crl check disable
#
wlan service-template 1 crypto
    ssid service
    bind WLAN-ESS 0
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
ssl server-policy eap-policy
    pki-domain do
#
eap-profile default-profile
    ssl-server-policy eap-policy
    method tls
    method peap-gtc
    user-credentials ldap-scheme ldap1
#
interface Vlan-interface100
    ip address 8.140.1.3 255.255.0.0
#
interface WLAN-ESS0
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
    port-security port-mode userlogin-secure-ext
    port-security tx-key-type 11key
    undo dot1x handshake
    dot1x mandatory-domain ldap
    undo dot1x multicast-trigger
#
wlan ap ap1 model WA2620E-AGN id 1
    serial-id 21023529G007C000020

```

```
radio 1
radio 2
    service-template 1
    radio enable
#
ip route-static 8.0.0.0 255.0.0.0 8.140.1.1
#
local-server authentication eap-profile default-profile
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 802.1X 与 RADIUS Offload 功能组合认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提 .....	1
3 配置举例 .....	1
3.1 组网需求 .....	1
3.2 配置思路 .....	2
3.3 配置注意事项 .....	2
3.4 配置步骤 .....	2
3.4.1 AC 的配置: .....	2
3.4.2 RADIUS server 的配置: .....	5
3.5 验证配置 .....	7
3.6 配置文件 .....	8
4 相关资料 .....	9

# 1 简介

本文档介绍当 RADIUS 服务器不支持 EAP 认证时，无线控制器采用 802.1X 的认证方式为 EAP 中继方式对无线客户端进行认证的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、802.1X 和 WLAN 特性。

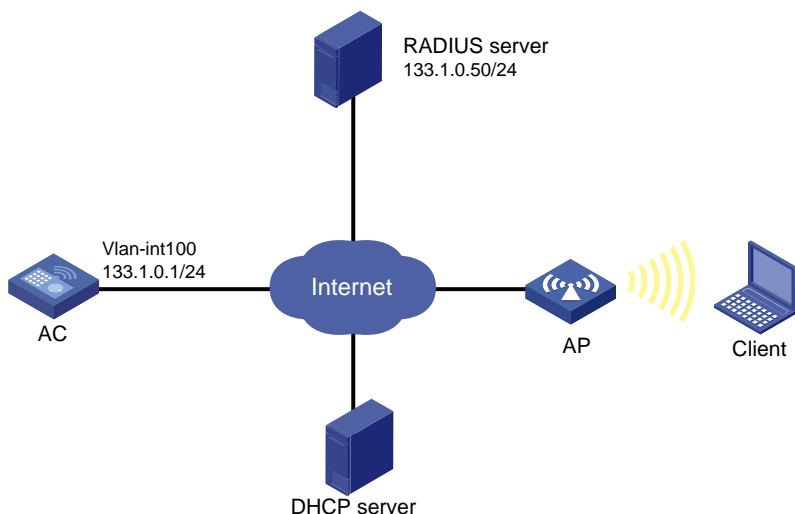
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，Client 和 AP 通过 DHCP 服务器分配 IP 地址，RADIUS 服务器不支持 EAP 认证，要求：

- 在 AC 上配置 802.1X 认证，以控制 Client 对网络资源的访问。
- 802.1X 认证方式采用 EAP 中继方式。
- 对 Client 和 AC 之间传输的数据进行加密，加密套件采用 AES-CCMP。
- 在强制认证域 dm0 进行认证。

图1 802.1X 与 RADIUS Offload 组合认证组网图



## 3.2 配置思路

- 由于需求中 RADIUS 服务器不支持 EAP 认证，要配置 EAP 中继方式的 802.1X 认证，需要使能 RADIUS Offload 功能。
- 要使能 RADIUS Offload 功能，必须配置本地 EAP 认证服务器，并指定其中的 EAP 认证方式为 PEAP-MSCHAPv2（目前仅支持此认证方式）。
- 当 EAP 认证方式为 PEAP-MSCHAPv2 时，必须设置用于 EAP 认证的 SSL 服务器端策略。
- 由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。
- 为了防止用户通过恶意假冒其它域账号从本端口接入网络，配置端口的强制认证域。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

## 3.4 配置步骤

### 3.4.1 AC 的配置：

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 133.1.0.1 255.255.255.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

#### (2) 配置无线接口

# 创建 WLAN-ESS 接口，并进入该视图。

```
[AC] interface wlan-ess 0
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS0] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS0] undo port hybrid vlan 1
[AC-WLAN-ESS0] port hybrid pvid vlan 200
[AC-WLAN-ESS0] port hybrid vlan 200 untagged
```

# 在 Hybrid 端口上使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS0] mac-vlan enable
[AC-WLAN-ESS0] quit
```

### (3) 配置无线服务

# 创建 crypto 类型的服务模板 1。

```
[AC] wlan service-template 1 crypto
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS0 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 0
```

# 使能 ccmp 加密套件。

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

# 使能无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### (4) 配置 AP 并绑定无线服务

# 在 AC 上配置 AP 名称为 ap1，型号名称这里选择 WA2620E-AGN，并配置序列号。

```
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 21023529G007C000020
```

# 将无线服务 1 绑定到射频 2。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

### (5) 配置 802.1X 并使能 EAP Offload 功能。

# 配置 RADIUS 方案为 eapoff，配置认证、计费 and 授权服务器的 IP 地址为 133.1.0.50，配置与认证、计费 and 授权服务器交互报文时的共享密钥均为 key。

```
[AC] radius scheme eapoff
[AC-radius-eapoff] primary authentication 133.1.0.50
[AC-radius-eapoff] primary accounting 133.1.0.50
[AC-radius-eapoff] key authentication key
[AC-radius-eapoff] key accounting key
```

# 使能 EAP Offload 功能。

```
[AC-radius-eapoff] eap offload method peap-mschapv2
[AC-radius-eapoff] quit
```

# 创建 ISP 域 dm0 域并进入其视图。

```
[AC] domain dm0
```



# 设置 ISP 域的认证、授权和计费方法均为 RADIUS 方式。

```
[AC-isp-dm0] accounting lan-access radius-scheme eapoff
[AC-isp-dm0] authentication lan-access radius-scheme eapoff
[AC-isp-dm0] authorization lan-access radius-scheme eapoff
[AC-isp-dm0] quit
```

# 启用端口安全，配置 802.1X 系统的认证方式为 EAP 中继方式。

```
[AC] port-security enable
[AC] dot1x authentication-method eap
```

# 进入 WLAN-ESS 接口视图。

```
[AC] interface wlan-ess 0
```

# 设置端口的安全模式为 userlogin-secure-ext。

```
[AC-WLAN-ESS0] port-security port-mode userlogin-secure-ext
```

# 在 WLAN-ESS 接口下使能 11key 类型的密钥协商功能。

```
[AC-WLAN-ESS0] port-security tx-key-type 11key
```

# 关闭在线用户握手功能和组播触发功能。

```
[AC-WLAN-ESS0] undo dot1x handshake
[AC-WLAN-ESS0] undo dot1x multicast-trigger
```

# 指定 WLAN-ESS 接口的认证域为 dm0。

```
[AC-WLAN-ESS0] dot1x mandatory-domain dm0
[AC-WLAN-ESS0] quit
```

## (6) 配置 SSL 服务器端策略

# 创建 PKI 实体 en，通用名 common。

```
[AC] pki entity en
[AC-pki-entity-en] common-name common
[AC-pki-entity-en] quit
```

# 创建 PKI 域 do，本端实体 en，注册机构：CA，不启用 CRL 查询。

```
[AC] pki domain do
[AC-pki-domain-do] certificate request from ca
[AC-pki-domain-do] certificate request entity en
[AC-pki-domain-do] crl check disable
[AC-pki-domain-do] quit
```

# 先用 FTP 等方式把证书上传到无线控制器中（详细过程略），再用命令导入证书。

```
[AC] pki import-certificate ca domain do pem filename root.pem
[AC] pki import-certificate local domain do p12 filename radius.p12
```

# 配置 SSL 服务器端策略 eap-policy，指定使用的 PKI 域为 do。

```
[AC] ssl server-policy eap-policy
[AC-ssl-server-policy-eap-policy] pki-domain do
[AC-ssl-server-policy-eap-policy] quit
```

## (7) 配置本地 EAP 认证

# 配置 EAP Profile，指定认证方法为 peap-mschapv2。

```
[AC] eap-profile default-profile
[AC-eap-prof-default-profile] ssl-server-policy eap-policy
[AC-eap-prof-default-profile] method peap-mschapv2
[AC-eap-prof-default-profile] quit
```

# 配置本地服务器认证所使用的 eap-profile 为 default-profile。

[AC] local-server authentication eap-profile default-profile

### 3.4.2 RADIUS server 的配置：



说明

下面以 iMC 为例 (使用 iMC 版本为: iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202) ), 说明 RADIUS 服务器的基本配置。

# 登录进入 iMC 管理平台, 选择“用户”页签, 单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项, 进入接入设备配置页面, 在该页面中单击<增加>按钮, 进入增加接入设备页面。

- 设置认证、计费共享密钥为 **key**, 其它保持缺省配置;
- 选择或手工增加接入设备, 添加 IP 地址为 133.1.0.1 的接入设备。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

接入配置			
认证端口 *	1812	计费端口 *	1813
组网方式	不启用混合组网	业务类型	LAN接入业务
接入设备类型	H3C(General)	接入设备分组	无
共享密钥 *	...	确认共享密钥 *	...
业务分组	未分组		

设备列表				
选择	手工增加	全部清除		
设备名称	设备IP地址	设备型号	备注	删除
	133.1.0.1			
共有1条记录。				

确定 取消

# 增加接入策略。

选择“用户”页签, 单击导航树中的[接入策略管理/接入策略管理]菜单项, 进入接入策略管理页面, 在该页面中单击<增加>按钮, 进入增加接入策略页面。设置接入策略名为 **office**, 其他均为默认配置即可。

图3 增加接入策略页面

用户 > 接入策略管理 > 接入策略管理 > 修改接入策略

基本信息

接入策略名 \*

office

业务分组 \*

未分组

描述

授权信息

接入时段

无

下行速率(Kbps)

优先级

证书认证

不启用

EAP证书认证

WAP证书认证

认证证书类型

EAP-TLS认证

下发VLAN

☐ 下发User Profile

☐ 下发ACL

分配IP地址 \*

否

上行速率(Kbps)

☐ 启用RSA认证

下发用户组

# 增加接入服务。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 设置服务名为 **office**；
- 选择缺省接入策略为 **office**，其他保持缺省配置。

图4 增加接入服务页面

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 \*

office

业务分组 \*

未分组

缺省安全策略 \*

不使用

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC-缺省页面 < PC

服务描述

☒ 可申请

服务后缀

缺省接入策略 \*

office

缺省内网外联配置 \*

不使用

☐ Portal无感知认证

接入场景列表

增加

名称	接入策略	安全策略	私有属性下发策略	内网外联配置	BYOD页面	优先级	修改	删除
未找到符合条件的记录。								

确定

取消

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 单击<增加用户>添加用户 **eapoff**，证件号码 **123456**；
- 添加帐号名为 **eapoff**，密码为 **123456**；
- 选中刚才配置的服务 **office**。

图5 增加接入用户

用户 > 接入用户 > 未分组 > 修改接入用户

接入用户

接入信息

用户姓名 \*

eapoff

帐号名 \*

eapoff

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

服务名	服务后缀	缺省安全策略	状态	分配IP地址
<input type="checkbox"/> 802.1x		不使用	可申请	
<input type="checkbox"/> 8705-eap		不使用	可申请	
<input type="checkbox"/> kt4166		不使用	可申请	
<input type="checkbox"/> lw_802.1x		不使用	可申请	
<input type="checkbox"/> mpc_ead		mpc_ead	可申请	
<input type="checkbox"/> mpc_peap		不使用	可申请	
<input checked="" type="checkbox"/> office		不使用	可申请	

3.5 验证配置

# Client 通过 AC 上线后，可以通过命令 **display connection** 查看到有 1 个用户在线。

```
[AC] display connection
Index=2      ,Username=eapoff@dm0
MAC=24-77-03-74-2C-C0
IP=N/A
IPv6=N/A
Total 1 connection(s) matched.
```

# 可以通过命令 **display connection ucibindex** 查看在线用户的详细信息。

```
[AC] display connection ucibindex 9
Index=9      , Username=eapoff@dm0
MAC=24-77-03-74-2C-C0
IP=N/A
IPv6=N/A
Access=8021X      ,AuthMethod=EAP
Port Type=Wireless-802.11,Port Name=WLAN-DBSS0:0
Initial VLAN=100, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
SessionTimeout=N/A, Terminate-Action=N/A
Start=2014-01-24 18:09:15 ,Current=2014-01-24 18:10:03 ,Online=00h00m48s
Total 1 connection matched.
```

## 3.6 配置文件

```
#
port-security enable
#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
ip address 133.1.0.1 255.255.255.0
#
radius scheme eapoff
primary authentication 133.1.0.50
primary accounting 133.1.0.50
key authentication cipher $c$3$9Q3c7agy84Q9YtZBkYcBKpNEqzjcIQ==
key accounting cipher $c$3$cSQELRJScdgMs6d7lJhB+mrJVwoiwQ==
eap offload method peap-mschapv2
#
domain dm0
authentication lan-access radius-scheme eapoff
authorization lan-access radius-scheme eapoff
accounting lan-access radius-scheme eapoff
access-limit disable
state active
idle-cut disable
self-service-url disable
#
pki entity en
common-name common
#
pki domain do
certificate request from ca
certificate request entity en
crl check disable
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 0
cipher-suite ccmp
security-ie rsn
service-template enable
#
ssl server-policy eap-policy
```

```

pki-domain do
#
eap-profile default-profile
  ssl-server-policy eap-policy
  method peap-mschapv2
#
interface WLAN-ESS0
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
  port-security port-mode userlogin-secure-ext
  port-security tx-key-type llkey
  undo dot1x handshake
  dot1x mandatory-domain dm0
  undo dot1x multicast-trigger
#
wlan ap ap1 model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
    service-template 1
  radio enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# H3C 无线控制器 IPv6 的 802.1X 远程认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提 .....	1
3 配置举例 .....	1
3.1 组网需求 .....	1
3.2 配置注意事项.....	2
3.3 配置步骤.....	2
3.3.1 配置 AC.....	2
3.3.2 配置 Switch.....	5
3.3.3 配置 RADIUS server.....	5
3.3.4 配置客户端.....	8
3.4 验证配置 .....	10
3.5 配置文件.....	12
4 相关资料 .....	14



# 1 简介

本文档介绍 IPv6 的 802.1X 远程认证典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V5 软件版本的无线控制器和接入点产品，不严格与具体硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、802.1X、WLAN 的相关特性。

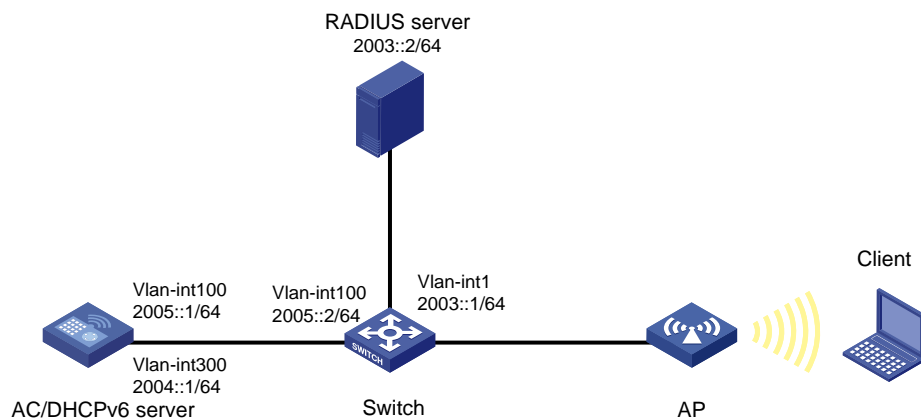
## 3 配置举例

### 3.1 组网需求

如图 1 所示组网，AC 作为 DHCPv6 server 为 AP 和 Client 分配 IPv6 地址，采用 iMC 作为 RADIUS 服务器对用户进行认证、授权和计费，要求：

- 对无线用户进行远程 802.1X 认证。
- 客户端链路层认证使用开放式系统认证。
- 通过配置客户端和 AP 之间的数据报文采用 802.1X 身份认证与密钥管理来确保用户数据的传输安全。
- 加密套件采用 CCMP。

图1 远程 802.1X 认证组网图



## 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 配置 AC

#### (1) 配置 AC 的接口

# 创建 VLAN 100 以及对应的 VLAN 接口，并为该接口配置 IPv6 地址。AP 将通过该 VLAN 与 AC 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 address 2005::1 64
```

# 取消对 RA 消息发布的抑制。

```
[AC-Vlan-interface100] undo ipv6 nd ra halt
```

# 设置被管理地址配置标志位为 1。

```
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

# 设置其他配置标志位为 1。

```
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。Client 将使用该 VLAN 接入无线网络。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ipv6 address 2004::1 64
```

# 取消对 RA 消息发布的抑制。

```
[AC-Vlan-interface300] undo ipv6 nd ra halt
```

# 设置被管理地址配置标志位为 1。

```
[AC-Vlan-interface300] ipv6 nd autoconfig managed-address-flag
```

# 设置其他配置标志位为 1。

```
[AC-Vlan-interface300] ipv6 nd autoconfig other-flag
[AC-Vlan-interface300] quit
```

# 配置 AC 与 Switch 相连的接口 GigabitEthernet1/0/1 的属性为 Trunk，允许 VLAN 100 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```

[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
(2) 配置 DHCPv6 server
# 全局使能 IPv6 功能。
[AC] ipv6
# 使能 DHCPv6 服务器功能。
[AC] ipv6 dhcp server enable
# 创建 DHCPv6 地址池 1，配置地址池范围为 2005::/64，为 AP 分配 IPv6 地址。
[AC] ipv6 dhcp pool 1
[AC-dhcp6-pool-1] network 2005::/64
[AC-dhcp6-pool-1] quit
# 创建 DHCPv6 地址池 2，配置地址池范围为 2004::/64，为 Client 分配 IPv6 地址。
[AC] ipv6 dhcp pool 2
[AC-dhcp6-pool-2] network 2004::/64
[AC-dhcp6-pool-2] quit
# 配置 VLAN 接口 100 引用地址池 1，为 AP 分配 IPv6 地址。
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 dhcp server apply pool 1
[AC-Vlan-interface100] quit
# 配置 VLAN 接口 300 引用地址池 2，为 Client 分配 IPv6 地址。
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ipv6 dhcp server apply pool 2
[AC-Vlan-interface300] quit
(3) 配置 RADIUS 方案
# 创建 RADIUS 方案 radius1 并进入其视图。
[AC] radius scheme radius1
# 配置主认证/计费 RADIUS 服务器的 IPv6 地址为 2003::2。
[AC-radius-radius1] primary authentication ipv6 2003::2
[AC-radius-radius1] primary accounting ipv6 2003::2
# 配置 AC 与认证/计费 RADIUS 服务器交互报文时的共享密钥为明文字符串 12345。
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。
[AC-radius-radius1] user-name-format without-domain
# 配置设备发送 RADIUS 报文使用的源 IPv6 地址为 2005::1。
[AC-radius-radius1] nas-ip ipv6 2005::1
[AC-radius-radius1] quit
(4) 配置认证域
# 创建名为 dom1 的 ISP 域并进入其视图。
[AC] domain dom1
# 配置 802.1X 用户使用 RADIUS 方案 radius1 进行认证、授权、计费。
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1

```

```

[AC-isp-dom1] quit
# 把配置的认证域 dom1 设置为系统缺省的 ISP 域。
[AC] domain default enable dom1
(5) 配置 802.1X 认证
# 使能端口安全。
[AC] port-security enable
# 配置 802.1X 系统的认证方法为 EAP。
[AC] dot1x authentication-method eap
# 创建 WLAN-ESS1 接口，并进入该视图。
[AC] interface wlan-ess 1
# 配置 WLAN-ESS1 接口类型为 Hybrid。
[AC-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 和 VLAN 300
不带 tag 通过。
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 300 untagged
# 开启 MAC-VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
# 配置端口的安全模式为 userLogin-SecureExt。
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
# 在接口 WLAN-ESS1 下使能 11key 类型的密钥协商功能。
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 关闭 802.1X 组播触发功能和在线用户握手功能。
[AC-WLAN-ESS1] undo dot1x multicast-trigger
[AC-WLAN-ESS1] undo dot1x handshake
[AC-WLAN-ESS1] quit
(6) 配置无线服务模板
# 创建 crypto 类型的服务模板 1，并进入无线服务模板视图。
[AC] wlan service-template 1 crypto
# 配置 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind WLAN-ESS 1
# 配置 CCMP 为加密套件，配 RSN 为安全信息元素。
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
# 使能无线服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
# 创建 AP，配置 AP 名称为 ap1，型号名称选择 WA4320H-ACN，并配置序列号
219801A0P69147G00098。
[AC] wlan ap ap1 model WA4320H-ACN
[AC-wlan-ap-ap1] serial-id 219801A0P69147G00098

```

# 进入 Radio 1 视图。

```
[AC-wlan-ap-ap1] radio 1
```

# 将无线服务模板 1 绑定到 radio 1,, 同时设置绑定到该射频的 VLAN 为 VLAN 300, 并开启射频。

```
[AC-wlan-ap-ap1-radio-1] service-template 1 vlan-id 300
```

```
[AC-wlan-ap-ap1-radio-1] radio enable
```

```
[AC-wlan-ap-ap1-radio-1] quit
```

```
[AC-wlan-ap-ap1] quit
```

(7) 配置 AC 到 RADIUS 服务器的静态路由

```
[AC] ipv6 route-static 2003:: 64 2005::2
```

### 3.3.2 配置 Switch

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 创建 VLAN 100 对应的 VLAN 接口, 并为该接口配置 IPv6 地址。

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] ipv6 address 2005::2 64
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

### 3.3.3 配置 RADIUS server



说明

- 下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.1、iMC UAM 7.1），说明 AAA 服务器的基本配置。
  - 在服务器上已经完成证书的安装。
- 

# 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入配置管理页面。在该页面中点击<增加>按钮，进入增加接入设备页面。

- 设置认证、计费共享密钥为 12345，其它保持缺省配置；
- 选择或手工增加 IPv6 接入设备，添加 IPv6 地址为 2005::1 的接入设备。

图2 增加接入设备页面

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

接入配置

认证端口 *	1812	计费端口 *	1813
组网方式	不启用混合组网	业务类型	LAN接入业务
接入设备类型	H3C(General)	业务分组	未分组
共享密钥 *	●●●●●	确认共享密钥 *	●●●●●
接入设备分组	无		

设备列表

选择 手工增加 增加IPv6设备 全部清除

设备名称	设备IP地址	设备型号	备注	删除
未找到符合条件的记录。				

#### # 增加接入策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击<增加>按钮，进入增加接入策略页面。

- 设置接入策略名输入 dot1x；
- 选择证书认证为 EAP 证书认证；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证。认证证书子类型需要与客户端的身份验证方法一致。

图3 增加服务策略页面

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 \*

dot1x

业务分组 \*

未分组

描述

授权信息

接入时段

无

下行速率(Kbps)

优先级

证书认证

☐ 不启用

☒ EAP证书认证

☐ WAPI证书认证

认证证书类型

EAP-PEAP认证

下发VLAN

☐ 下发User Profile

☐ 下发ACL

分配IP地址 \*

否

上行速率(Kbps)

☐ 启用RSA认证

认证证书子类型

MS-CHAPV2认

下发用户组

# 增加接入服务。

选择“用户”页签，单击导航树[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 设置服务名为 dot1x;
- 设置缺省接入策略为已经创建的 dot1x 策略。

图4 增加接入服务页面

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 \*

dot1x

业务分组 \*

未分组

缺省安全策略 \*

不使用

缺省私有属性下发策略 \*

不使用

缺省单帐号最大绑定终端数 \*

0

服务描述

☒ 可申请

☐ Portal无感知认证

服务后缀

缺省接入策略 \*

dot1x

缺省内网外连策略 \*

不使用

缺省单帐号在线数量限制 \*

0

接入场景列表

增加

名称	接入策略	安全策略	私有属性下发策略	内网外连策略	优先级	修改	删除
未找到符合条件的记录。							

确定

取消

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 添加用户 user;

- 添加账号名为 **dot1x**，密码为 **dot1x123**；
- 选中之前配置的服务 **dot1x**。

图5 增加接入用户页面

用户 > 接入用户 > 增加接入用户

接入用户

接入信息

用户姓名 \*

user

选择

增加用户

帐号名 \*

dot1x

☐ 预开用户

☐ 缺省BYOD用户

☐ MAC地址认证用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数 \*

1

<input type="checkbox"/>	dot1x		不使用	可申请
<input checked="" type="checkbox"/>	dot1x		不使用	可申请
<input type="checkbox"/>	dotpap		不使用	可申请

3.3.4 配置客户端

# 打开手机，选择 SSID 为 **service** 无线服务进行连接，然后输入无线网络信息。

- EAP 方法选择 **PEAP**；
- 身份输入 **dot1x**；
- 密码输入 **dot1x123**；
- 其它保持缺省配置，然后单击“连接”。



图6 连接无线网络

中国移动 ...

19:34

70%

取消

输入密码

连接

EAP 方法

PEAP >

阶段 2 身份验证

无 >

CA 证书

无 >

身份 dot1x

×

匿名身份

密码 dot1x123

×

☒ 显示密码

图7 无线网络连接成功



### 3.4 验证配置

# 当用户通过认证连接到 AP 后，可以在 AC 上使用 **display connection** 查看有 1 个用户在线。

```
[AC] display connection
Index=1      ,Username=dot1x@dom1
MAC=38-29-5A-40-95-89
IP=N/A
IPv6=N/A
Online=00h09m55s
Total 1 connection(s) matched.
```

# 在 AC 上使用 **display connection ucibindex** 查看用户的较详细信息。

```
[AC] display connection ucibindex 1
Index=1      , Username=dot1x@dom1
MAC=38-29-5A-40-95-89
IP=N/A
IPv6=N/A
Access=8021X      ,AuthMethod=EAP
Port Type=Wireless-802.11,Port Name=WLAN-DBSS1:0
Initial VLAN=300, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
```

```
Traffic Statistic:
    InputOctets    =5122      OutputOctets    =3059
    InputGigawords=0      OutputGigawords=0
Priority=Disable
SessionTimeout=86400(s), Terminate-Action=Radius-Request
Start=2018-09-18 17:58:24 ,Current=2018-09-18 18:09:54 ,Online=00h11m30s
Total 1 connection matched.
```

# 在 AC 上可以通过 **display wlan client verbose** 命令查看客户端上线情况。

```
[AC] display wlan client verbose
```

```
Total Number of Clients      : 1
                               Client Information
```

```
-----
MAC Address                   : 3829-5a40-9589
User Name                     : dot1x
IP Address                    : 0.0.0.0
IPv6 Address                  : -NA-
AID                           : 1
AP Name                       : ap1
Radio Id                      : 1
Antenna Id                    : 0
Service Template Number      : 1
SSID                          : service
BSSID                         : 70ba-ef07-c560
Port                          : WLAN-DBSS1:0
VLAN                          : 300
State                         : Running
Power Save Mode               : Active
Wireless Mode                 : 11an
Channel Band-width            : 20/40MHz
SM Power Save Enable          : Enabled
SM Power Save Mode            : Static
Short GI for 20MHz             : Supported
Short GI for 40MHz            : Supported
LDPC                          : Not Supported
STBC TX capability            : Not Supported
STBC RX capability            : Supported
Support MCS Set               : 0,1,2,3,4,5,6,7
BLOCK ACK-TID 0               : BOTH
QoS Mode                      : WMM
Listen Interval (Beacon Interval) : 2
RSSI                          : 42
Rx/Tx Rate                    : 135/6
Client Type                   : WPA2(RSN)
Authentication Method          : Open System
Authentication Mode            : Central
AKM Method                    : Dot1X
Key Derivation                 : SHA1
4-Way Handshake State         : PTKINITDONE
```

```
Group Key State          : IDLE
Encryption Cipher        : AES-CCMP
PMF Status               : -NA-
Roam Status              : Normal
Roam Count               : 0
Up Time (hh:mm:ss)      : 00:00:16
Bonjour Records          :
```

-----

## 3.5 配置文件

- AC:

```
#
domain default enable dom1
#
ipv6
#
port-security enable
#
dot1x authentication-method eap
#
ipv6 dhcp server enable
#
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme radius1
primary authentication ipv6 2003::0002
primary accounting ipv6 2003::0002
key authentication cipher $c$3$VPHT6uKFirHoAE/1NuWT0iB3sfHK8WAF
key accounting cipher $c$3$WmKcjQoQnrkKbi88ghZndPgV1N76gF94
user-name-format without-domain
nas-ip ipv6 2005::0001
#
domain dom1
authentication lan-access radius-scheme radius1
authorization lan-access radius-scheme radius1
accounting lan-access radius-scheme radius1
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 1
cipher-suite ccmp
```

```

security-ie rsn
service-template enable
#
ipv6 dhcp pool 1
network 2005::/64
#
ipv6 dhcp pool 2
network 2004::/64
#
interface Vlan-interface100
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
ipv6 address 2005::1/64
ipv6 dhcp server apply pool 1
#
interface Vlan-interface300
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
ipv6 address 2004::1/64
ipv6 dhcp server apply pool 2
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 300
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 300 untagged
port hybrid pvid vlan 200
mac-vlan enable
port-security port-mode userlogin-secure-ext
port-security tx-key-type 11key
undo dot1x handshake
undo dot1x multicast-trigger
#
wlan ap ap1 model WA4320H-ACN id 1
serial-id 219801A0P69147G00098
radio 1
service-template 1 vlan-id 300
radio enable
#
ipv6 route-static 2003:: 64 2005::2
#
return

```

- Switch:

```
#
vlan 1
#
vlan 100
#
vlan 300
#
interface Vlan-interface1
    ipv6 address 2003::1/64
#
interface Vlan-interface100
    ipv6 address 2005::2/64
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 300
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
    port access vlan 100
    poe enable
#
return
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 通过 802.1X 认证服务器动态下发授权 ACL 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

1 简介.....	1
2 配置前提 .....	1
3 802.1X 认证通过 Windows Server 2003 IAS 服务器下发 ACL 配置举例 .....	1
3.1 组网需求 .....	1
3.2 配置思路 .....	1
3.3 配置注意事项.....	2
3.4 配置步骤 .....	2
3.4.1 AC 的配置 .....	2
3.4.2 Switch 的配置 .....	5
3.4.3 Windows Server 2003 IAS 服务器的配置 .....	5
3.5 验证配置 .....	11
3.6 配置文件 .....	12
4 802.1X 认证通过 iMC 服务器下发 ACL 配置举例 .....	14
4.1 组网需求 .....	14
4.2 配置思路 .....	14
4.3 配置注意事项.....	15
4.4 配置步骤 .....	15
4.4.1 AC 的配置 .....	15
4.4.2 Switch 的配置 .....	18
4.4.3 iMC 服务器的配置 .....	19
4.5 验证配置 .....	21
4.6 配置文件 .....	23
5 相关资料 .....	25



# 1 简介

本文档介绍无线控制器通过 802.1X 认证服务器动态下发授权 ACL 的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、WLAN、802.1X 特性。

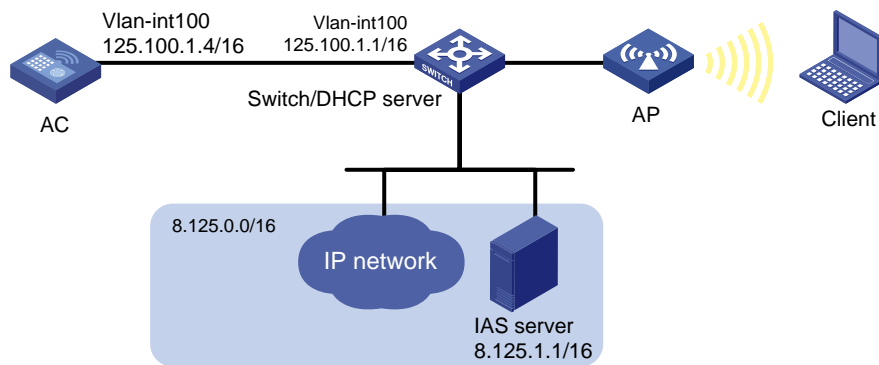
## 3 802.1X 认证通过 Windows Server 2003 IAS 服务器下发 ACL 配置举例

### 3.1 组网需求

如图 1 所示，Windows Server 2003 IAS 服务器作为 RADIUS 服务器，对 Client 进行认证并下发授权 ACL。具体应用需求如下：

- Client 需要通过 802.1X 认证才能上线；
- Client 通过认证后允许访问网络 8.125.0.0/16，不允许访问其他网络资源。
- 防止用户通过恶意假冒其它域账号从本端口接入网络。

图1 授权 ACL 下发典型配置组网图



### 3.2 配置思路

- 为了实现 Windows Server 2003 IAS 服务器下发授权 ACL，需要在用户使用的“远程访问策略”中添加 Filter-ID 属性。
- 由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。

- 对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。
- 为了防止用户通过恶意假冒其它域账号从本端口接入网络，配置端口的强制认证域。

### 3.3 配置注意事项

- Windows Server 2003 IAS 服务器授权下发的 ACL 必须是 AC 设备上已经配置的 ACL，且 ACL 的内容不能为空，否则 802.1X 无法认证成功。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

### 3.4 配置步骤

#### 3.4.1 AC 的配置

##### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道且 AC 通过 VLAN 100 与 RADIUS 服务器通信。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 125.100.1.4 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

##### (2) 配置 ACL

# 创建 ACL 3000。

```
[AC] acl number 3000
```

# 定义规则 0，允许目的地址为 8.125.0.0/16 的报文通过。

```
[AC-acl-adv-3000] rule 0 permit ip destination 8.125.0.0 0.0.255.255
```

# 定义规则 1，禁止任何 IP 报文通过。

```
[AC-acl-adv-3000] rule 1 deny ip
```

```
[AC-acl-adv-3000] quit
```

### (3) 配置 802.1X 认证

# 全局模式下使能端口安全。

```
[AC] port-security enable
```

# 选择 802.1X 认证方式为 EAP。

```
[AC] dot1x authentication-method eap
```

### (4) 配置认证策略

# 创建 RADIUS 方案 office 并进入其视图。

```
[AC] radius scheme office
```

# 配置 RADIUS 方案服务类型为扩展型。

```
[AC-radius-office] server-type extended
```

# 设置主认证 RADIUS 服务器的 IP 地址 8.125.1.1。

```
[AC-radius-office] primary authentication 8.125.1.1
```

# 设置主计费 RADIUS 服务器的 IP 地址 8.125.1.1。

```
[AC-radius-office] primary accounting 8.125.1.1
```

# 设置系统与认证 RADIUS 服务器交互报文时的共享密钥为 123456。

```
[AC-radius-office] key authentication 123456
```

# 设置系统与计费 RADIUS 服务器交互报文时的共享密钥为 123456。

```
[AC-radius-office] key accounting 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带域名。

```
[AC-radius-office] user-name-format without-domain
```

# 设置设备发送 RADIUS 报文时使用的源 IP 地址 125.100.1.4。

```
[AC-radius-radius] nas-ip 125.100.1.4
```

```
[AC-radius-radius] quit
```

### (5) 配置认证域

# 创建 office 域并进入其视图。

```
[AC] domain office
```

# 为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] authentication lan-access radius-scheme office
```

# 为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] authorization lan-access radius-scheme office
```

# 为 lan-access 用户配置计费为 none，不计费。

```
[AC-isp-office] accounting lan-access none
```

```
[AC-isp-office] quit
```

### (6) 配置无线接口

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
```

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置 WLAN-ESS1 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
# 使能 MAC-VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
# 在 WLAN-ESS1 口上配置端口安全，选用 802.1X 认证方式。
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 关闭 802.1x 握手功能
[AC-WLAN-ESS1] undo dot1x handshake
# 关闭 802.1x 多播触发功能
[AC-WLAN-ESS1] undo dot1x multicast-trigger
# 在 WLAN-ESS1 端口上指定 802.1X 认证的强制认证域为 office。
[AC-WLAN-ESS1] dot1x mandatory-domain office
[AC-WLAN-ESS1] quit
```

#### (7) 配置无线服务

```
# 创建 crypto 类型的服务模板 1。
[AC] wlan service-template 1 crypto
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 配置加密套件为 CCMP。
[AC-wlan-st-1] cipher-suite ccmp
# 配置安全信息元素为 RSN。
[AC-wlan-st-1] security-ie rsn
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

#### (8) 配置射频接口并绑定服务模板

```
# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN，并配置 AP 的序列号。
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的服务模板 1 与射频 2 进行关联，Client 通过服务模板 1 接入 VLAN 300。
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

#### (9) 配置 AC 的默认路由

```
# 将 AC 的默认路由指向交换机，地址为 125.100.1.1
[AC] ip route-static 0.0.0.0 0.0.0.0 125.100.1.1
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 trunk, 当前 trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 access, 并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 使能 DHCP 服务。

```
[Switch] dhcp enable
```

# 创建名为 vlan100 的 DHCP 地址池, 配置地址池范围为 125.100.1.10~125.100.1.20, 网关地址为 125.100.1.4, 为 AP 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan100 extended
[Switch-dhcp-pool-vlan100] network ip range 125.100.1.10 125.100.1.20
[Switch-dhcp-pool-vlan100] network mask 255.255.0.0
[Switch-dhcp-pool-vlan100] gateway-list 125.100.1.4
[Switch-dhcp-pool-vlan100] quit
```

# 创建名为 vlan300 的 DHCP 地址池, 配置地址池范围为 125.30.0.2~125.30.0.5, 网关地址为 125.30.0.6, 为 Client 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan300 extended
[Switch-dhcp-pool-vlan300] network ip range 125.30.0.2 125.30.0.5
[Switch-dhcp-pool-vlan300] network mask 255.255.0.0
[Switch-dhcp-pool-vlan300] gateway-list 125.30.0.6
[Switch-dhcp-pool-vlan300] quit
```

### 3.4.3 Windows Server 2003 IAS 服务器的配置

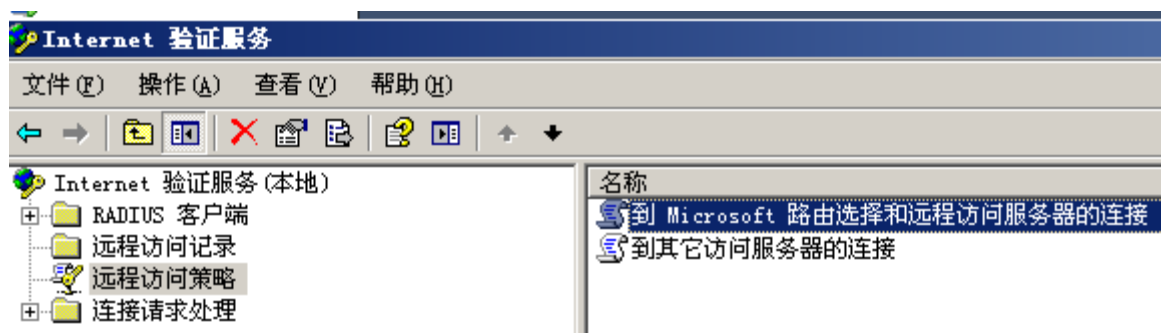
# 如图 2 所示, 单击“开始”菜单, 选择[管理工具/Internet 验证服务]菜单项, 单击进入“Internet 验证服务”。

图2 进入 Internet 验证服务



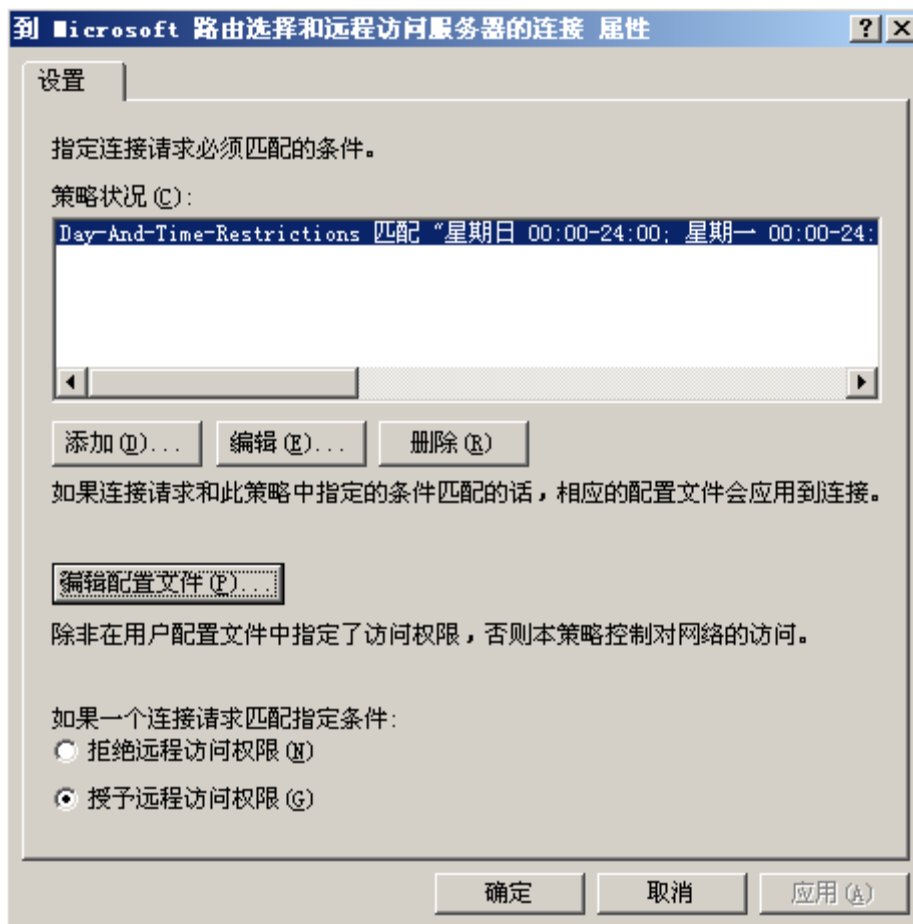
# 如图3所示，在左边菜单中单击“远程访问策略”标签，选择“到 Microsoft 路由选择和远程访问服务器的连接”，双击进入。

图3 选择远程访问策略



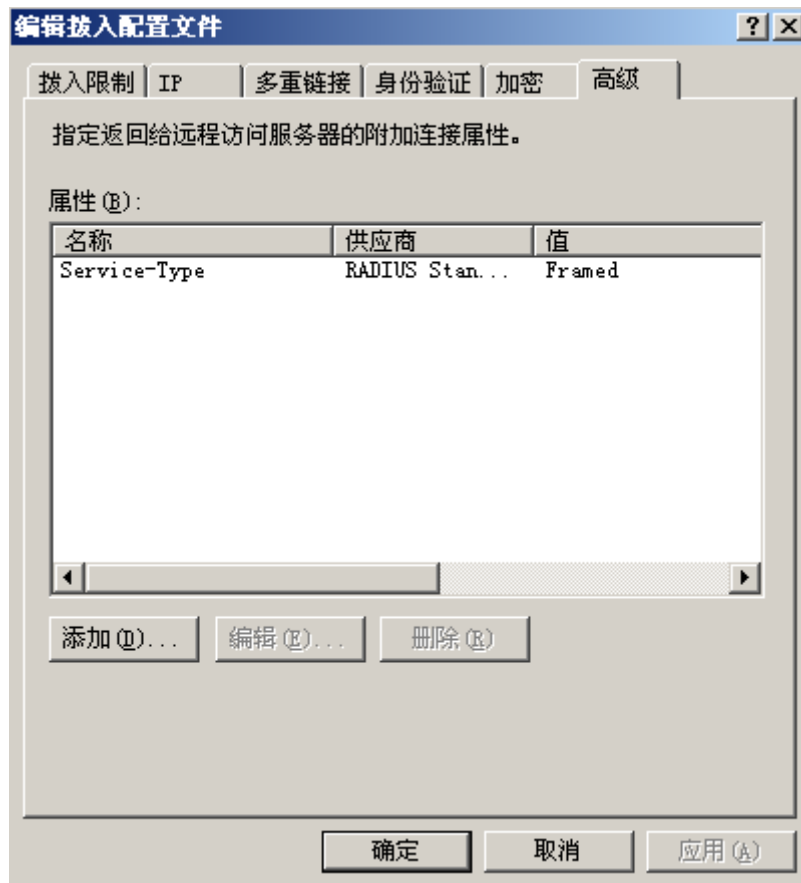
# 如图4所示，点击<编辑配置文件>按钮，编辑用户的访问策略。

图4 编辑用户使用的远程策略的配置文件



# 如图 5 所示，选取“高级”页签，点击<添加>按钮，弹出“添加属性”窗口。

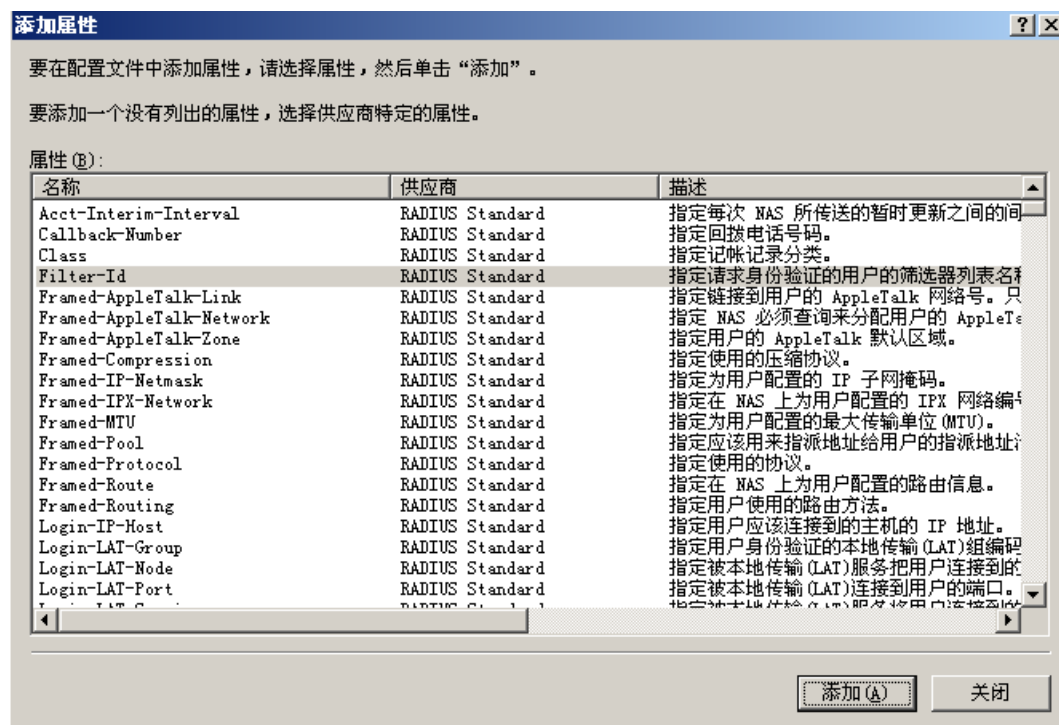
图5 编辑拨入配置文件



# 如图6所示，选取 Filter-ID 选项，双击 Filter-ID，弹出“多值属性信息”对话框。

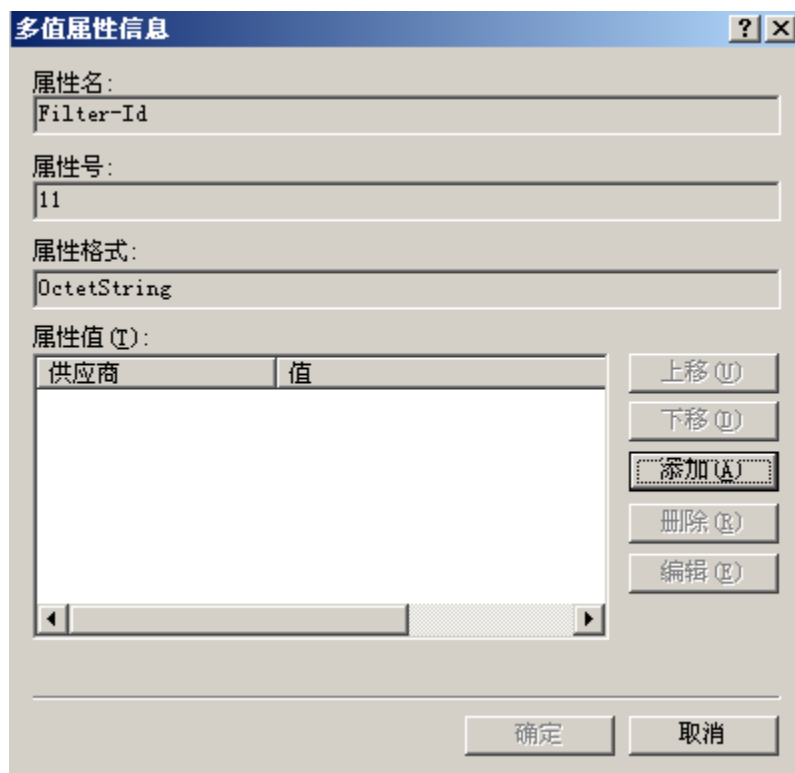


图6 添加 Filter-ID 属性



# 如图 7 所示，在“多值属性信息”对话框中点击<添加>按钮，弹出“属性信息”窗口。

图7 添加多值属性信息



# 如图 8 所示，在“属性信息”窗口中配置 Filter-ID 属性值。选择字符串形式，输入值 3000，表示下发序号为 3000 的 ACL，单击<确定>按钮，完成属性添加。

图8 在属性信息中添加所要下发的 ACL

属性信息

属性名:  
Filter-Id

属性号:  
11

属性格式:  
OctetString

输入属性值所用的格式 (E): ☒ 字符串 (S) ☐ 十六进制 (H)

3000

确定 取消

# 完成属性添加后如下，点击<应用>按钮，然后点击<确定>按钮，完成操作。

图9 添加属性完成

编辑拨入配置文件

拨入限制 IP 多重链接 身份验证 加密 高级

指定返回给远程访问服务器的附加连接属性。

属性 (E):

名称	供应商	值
Service-Type	RADIUS Stan...	Framed
Filter-Id	RADIUS Stan...	3000

添加 (A)... 编辑 (E)... 删除 (D)

确定 取消 应用 (A)

## 3.5 验证配置

- (1) Client 通过 802.1X 认证上线后，执行 **display connection** 命令，查看 802.1X 用户上线后的基本信息。观察上线信息的 Index，本例中 Index 值为 27。

```
<AC> display connection
Index=27 ,Username=lw@office
MAC=00-24-01-EB-FA-EE
IP=N/A
IPv6=N/A
Online=00h00m09s
Total 1 connection(s) matched.
```

- (2) 通过执行 **display connection ucibindex 27** 命令，得到 Client 通过 802.1X 认证后的详细信息，可以查看到授权 ACL 下发成功。

```
<AC> display connection ucibindex 27
Index=27 , Username=lw@office
MAC=00-24-01-EB-FA-EE
IP=N/A
IPv6=N/A
Access=8021X ,AuthMethod=EAP
Port Type=Wireless-802.11,Port Name=WLAN-DBSS1:0
Initial VLAN=200, Authorization VLAN=N/A
ACL Group=3000
User Profile=N/A
CAR=Disable
Traffic Statistic:
    InputOctets    =0          OutputOctets    =0
    InputGigawords=0          OutputGigawords=0
Priority=Disable
SessionTimeout=N/A, Terminate-Action=N/A
Start=2013-11-20 19:34:23 ,Current=2013-11-20 19:34:38 ,Online=00h00m15s
Total 1 connection matched.
```

- (3) Client 认证成功并获取 IP 地址后，能 ping 通 8.125.0.0/16 网段，无法 ping 通其他网段，证明授权 ACL 已生效。

```
C:\Documents and Settings\Administrator>ping 8.125.1.1
```

```
Pinging 8.125.1.1 with 32 bytes of data:
```

```
Reply from 8.125.1.1: bytes=32 time=6ms TTL=254
Reply from 8.125.1.1: bytes=32 time=12ms TTL=254
Reply from 8.125.1.1: bytes=32 time=46ms TTL=254
Reply from 8.125.1.1: bytes=32 time=25ms TTL=254
```

```
Ping statistics for 8.125.1.1:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 46ms, Average = 22ms
```

```
C:\Documents and Settings\Administrator>ping 125.100.1.1
```

```
Pinging 125.100.1.1 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 125.100.1.1:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(4) 通过 **display acl** 命令可以查看到 ACL 3000 规则的匹配数量（略）。

## 3.6 配置文件

```
#
port-security enable
#
dot1x authentication-method eap
#
acl number 3000
rule 0 permit ip destination 8.125.0.0 0.0.255.255
rule 1 deny ip
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
server-type extended
primary authentication 8.125.1.1
primary accounting 8.125.1.1
key authentication cipher $c$3$EnNB6wxpjYSAJMiU2aaeNArZaBzSA13G5A==
key accounting cipher $c$3$o9Wa5f+anDJ56GonM91E7c8otvLF06HKGA==
user-name-format without-domain
nas-ip 125.100.1.4
#
domain office
authentication lan-access radius-scheme office
authorization lan-access radius-scheme office
accounting lan-access none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
```

```

wlan service-template 1 crypto
  ssid service
  bind WLAN-ESS 1
  cipher-suite ccmp
  security-ie rsn
  service-template enable
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200 300
#
interface Vlan-interface100
  ip address 125.100.1.4 255.255.0.0
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
  port-security port-mode userlogin-secure-ext
  port-security tx-key-type llkey
  undo dot1x handshake
  dot1x mandatory-domain office
  undo dot1x multicast-trigger
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
  service-template 1 vlan-id 300
  radio enable
#
ip route-static 0.0.0.0 0.0.0.0 125.100.1.1
#
•   Switch:
#
  dhcp enable
#
  vlan 100
#
  vlan 300
#
  dhcp server ip-pool vlan100 extended
  network ip range 125.100.1.10 125.100.1.20
  network mask 255.255.0.0
  gateway-list 125.100.1.4
#

```

```

dhcp server ip-pool vlan300 extended
network ip range 125.30.0.2 125.30.0.5
network mask 255.255.0.0
gateway-list 125.30.0.6
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
poe enable
#

```

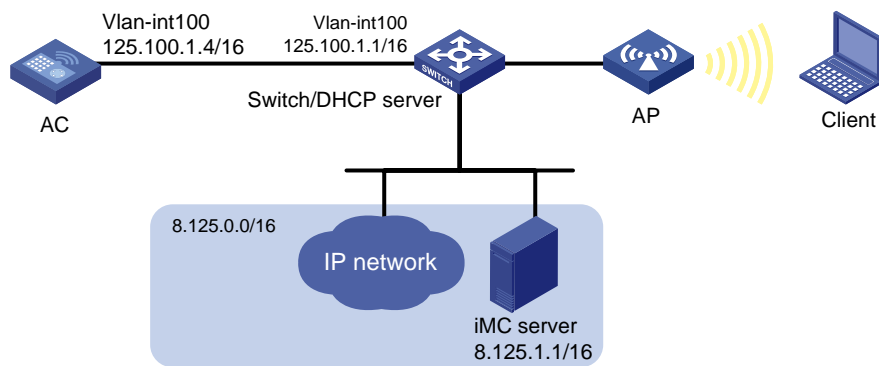
## 4 802.1X 认证通过 iMC 服务器下发 ACL 配置举例

### 4.1 组网需求

如图 10 所示，iMC 服务器作为 RADIUS 服务器，对 Client 进行认证并下发授权 ACL。具体应用需求如下：

- Client 需要通过 802.1X 认证才能上线；
- Client 通过认证后允许访问网络 8.125.0.0/16，其他网络资源不允许访问。
- 防止用户通过恶意假冒其它域账号从本端口接入网络。

图10 授权 ACL 下发典型配置组网图



### 4.2 配置思路

- 由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。

- 对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。
- 为了防止用户通过恶意假冒其它域账号从本端口接入网络，配置端口的强制认证域。

## 4.3 配置注意事项

- iMC 服务器授权下发的 ACL 必须是 AC 设备上已经配置的 ACL，且 ACL 的内容不能为空，否则 802.1X 无法认证成功。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

## 4.4 配置步骤

### 4.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道，且 AC 通过 VLAN 100 与 RADIUS 服务器通信。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 125.100.1.4 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口配置使用的 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为无线用户接入 VLAN，RADIUS 服务器会下发 VLAN 300 作为授权 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 ACL

# 创建 ACL 3000。

```
[AC] acl number 3000
```

# 定义规则 0，允许目的地址为 8.125.0.0/16 的报文通过。

```
[AC-acl-adv-3000] rule 0 permit ip destination 8.125.0.0 0.0.255.255
```

# 定义规则 1，禁止任何 IP 报文通过。

```
[AC-acl-adv-3000] rule 1 deny ip
```

```
[AC-acl-adv-3000] quit
```

### (3) 配置 802.1X 认证

# 全局模式下使能端口安全。

```
[AC] port-security enable
```

# 选择 802.1X 认证方式为 EAP。

```
[AC] dot1x authentication-method eap
```

### (4) 配置认证策略

# 创建 RADIUS 方案 office 并进入其视图。

```
[AC] radius scheme office
```

# 配置 RADIUS 方案服务类型为扩展型。。

```
[AC-radius-office] server-type extended
```

# 设置主认证 RADIUS 服务器的 IP 地址 8.125.1.1。

```
[AC-radius-office] primary authentication 8.125.1.1
```

# 设置主计费 RADIUS 服务器的 IP 地址 8.125.1.1。

```
[AC-radius-office] primary accounting 8.125.1.1
```

# 设置系统与认证 RADIUS 服务器交互报文时的共享密钥为 123456。

```
[AC-radius-office] key authentication 123456
```

# 设置系统与计费 RADIUS 服务器交互报文时的共享密钥为 123456。

```
[AC-radius-office] key accounting 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带域名。

```
[AC-radius-office] user-name-format without-domain
```

# 设置设备发送 RADIUS 报文时使用的源 IP 地址 125.100.1.4。

```
[AC-radius-radius] nas-ip 125.100.1.4
```

```
[AC-radius-radius] quit
```

### (5) 配置认证域

# 创建 office 域并进入其视图。

```
[AC] domain office
```

# 为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] authentication lan-access radius-scheme office
```

# 为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] authorization lan-access radius-scheme office
```

# 为 lan-access 用户配置计费方案为 none，不计费。

```
[AC-isp-office] accounting lan-access none
```

```
[AC-isp-office] quit
```

### (6) 配置无线接口，使能端口安全

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
```

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置 WLAN-ESS1 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```



```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
# 使能 MAC-VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
# 在 WLAN-ESS1 口上配置端口安全，选用 802.1X 认证方式。
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 关闭 802.1X 握手功能
[AC-WLAN-ESS1] undo dot1x handshake
# 关闭 802.1X 多播触发功能
[AC-WLAN-ESS1] undo dot1x multicast-trigger
# 在 WLAN-ESS1 端口上指定 802.1X 认证的强制认证域为 office。
[AC-WLAN-ESS1] dot1x mandatory-domain office
[AC-WLAN-ESS1] quit
```

### (7) 配置无线服务

```
# 创建 crypto 类型的服务模板 1。
[AC] wlan service-template 1 crypto
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 配置加密套件为 CCMP。
[AC-wlan-st-1] cipher-suite ccmp
# 配置安全信息元素为 RSN。
[AC-wlan-st-1] security-ie rsn
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### (8) 配置射频接口并绑定服务模板

```
# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN，并配置 AP 的序列号。
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的服务模板 1 与射频 2 进行关联，且 Client 通过服务模板 1 接入 VLAN 300。
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

### (9) 配置 AC 的默认路由

```
# 将 AC 的默认路由指向交换机，地址为 125.100.1.1
[AC] ip route-static 0.0.0.0 0.0.0.0 125.100.1.1
```

## 4.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 trunk, 当前 trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 access, 并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 使能 DHCP 服务。

```
[Switch] dhcp enable
```

# 创建名为 vlan100 的 DHCP 地址池, 配置地址池范围为 125.100.1.10~125.100.1.20, 网关地址为 125.100.1.4, 为 AP 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan100 extended
[Switch-dhcp-pool-vlan100] network ip range 125.100.1.10 125.100.1.20
[Switch-dhcp-pool-vlan100] network mask 255.255.0.0
[Switch-dhcp-pool-vlan100] gateway-list 125.100.1.4
[Switch-dhcp-pool-vlan100] quit
```

# 创建名为 vlan300 的 DHCP 地址池, 配置地址池范围为 125.30.0.2~125.30.0.5, 网关地址为 125.30.0.6, 为 Client 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan300 extended
[Switch-dhcp-pool-vlan300] network ip range 125.30.0.2 125.30.0.5
[Switch-dhcp-pool-vlan300] network mask 255.255.0.0
[Switch-dhcp-pool-vlan300] gateway-list 125.30.0.6
[Switch-dhcp-pool-vlan300] quit
```

### 4.4.3 iMC 服务器的配置



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.2(E0401)、iMC UAM 5.2(E0402)），说明 RADIUS 服务器的基本配置。

# 增加接入设备。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[接入用户管理/接入设备管理/接入设备配置]菜单项，单击“增加”按钮，进入“增加接入设备”页面，单击<手工增加>按钮，进入“手工增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 125.100.1.4 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图11 增加接入设备

业务 >> 用户接入管理 >> 接入设备管理 >> 接入设备配置 >> 增加接入设备

**接入配置**

认证端口	1812	计费端口	1813
共享密钥	*****	确认共享密钥	*****
接入区域	无	业务类型	LAN接入业务
接入设备类型	H3C(General)	组网方式	不启用混合组网
业务分组	未分组		

**设备列表**

选择 手工增加 全部清除

共有1条记录。

设备名称	设备IP地址	设备型号	备注	删除
	125.100.1.4			X

确定 取消

# 增加接入规则配置。

选择“业务”页签，单击导航树中的[用户接入管理/接入规则管理]菜单项，单击<增加>按钮，创建一条接入规则。

- 接入规则名输入“office”。
- 授权信息中证书模式选择 EAP 证书认证，与 AC 上 802.1X 的认证保持一致。
- 认证证书类型选择 EAP-PEAP。
- 下发 ACL 选择 3000。

其它参数采用缺省值，并单击<确定>按钮完成操作。

图12 增加接入规则

业务 >> 用户接入管理 >> 接入规则管理 >> 增加接入规则

基本信息

\* 接入规则名

office

\* 业务分组

未分组

描述

授权信息

接入时段

无

下行速率

Kbps

优先级

证书认证

☐ 不启用

☒ EAP证书认证

☐ WAPI证书认证

认证证书类型

EAP-PEAP认证

下发VLAN

☐ 下发User Profile

☒ 下发ACL

☒ 手工输入

3000

☐ 列表选择

☐ 接入ACL列表

\* 分配IP地址

否

上行速率

Kbps

☐ 启用RSA认证

认证证书子类型

MS-CHAPV2认证

下发用户组

# 增加接入服务配置。

选择“业务”页签，单击导航树中的[用户接入管理/服务配置管理]菜单项，单击<增加>按钮，创建一条接入服务。

- 服务名输入“1x\_ACL”。
- 缺省接入规则选择“office”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图13 添加服务配置

业务 >> 用户接入管理 >> 服务配置管理 >> 增加服务配置

基本信息

\* 服务名

1x\_ACL

服务后缀

\* 业务分组

未分组

\* 缺省接入规则

office

\* 缺省私有属性下发策略

不使用

计费策略

不计费

服务描述

☒ 可申请

☐ Portal智能终端快速认证

接入策略列表

增加

接入场景	接入规则	私有属性下发策略	优先级	修改	删除
------	------	----------	-----	----	----

确定


取消

# 增加用户配置。

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户/接入用户列表]菜单项，单击<增加>按钮，增加一个接入用户。

- 单击“增加用户”。
- 用户姓名输入“lw”。
- 证件号码输入“lw”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图14 iMC 上增加用户

 用户 >> 增加用户 ? 帮助

增加用户

基本信息

\* 用户姓名

lw

\* 证件号码

lw

通讯地址

电话


?

电子邮件

?

\* 用户分组

未分组



☐ 开通自助帐户

确定

取消

- # 增加接入用户配置。
- 选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户/接入用户列表]菜单项，单击<增加>按钮，增加一个接入用户。
- 账号名输入“lw”。
  - 密码与密码确认输入“1x\_ACL”。
  - 选择服务名“1x\_ACL”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图15 给用户绑定接入服务

 用户 >> 所有接入用户 >> 增加接入用户

接入用户

接入信息

\* 用户姓名

lw

选择

增加用户

\* 帐号名

lw

☐ 预开用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

\* 密码

.....

\* 密码确认

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

失效日期

Portal智能终端最大绑定数

1

最大闲置时长

分钟

在线数量限制

1

帐号类型

预付费

\* 预付金额

0

元

自助充值

允许

登录提示信息

接入服务

	服务名	服务后缀	状态	计费策略	分配IP地址
<input checked="" type="checkbox"/>	1x_ACL		可申请	不计费	
<input type="checkbox"/>	office	office	可申请	不计费	

4.5 验证配置

- (1) Client 通过 802.1X 认证上线后，执行 **display connection** 命令，查看 802.1X 用户上线后的基本信息。观察上线信息的 Index，本例中 Index 值为 33。
- ```
<AC> display connection
Index=33 ,Username=lw@office
```

MAC=00-24-01-EB-FA-EE

IP=N/A

IPv6=N/A

Online=00h00m09s

Total 1 connection(s) matched.

- (2) 通过执行 **display connection ucibindex 33** 命令，得到 Client 通过 802.1X 认证后的详细信息。可以查看到 iMC 服务器下发授权 ACL 成功。

```
<AC> display connection ucibindex 33
```

Index=27 , Username=lw@office

MAC=00-24-01-EB-FA-EE

IP=N/A

IPv6=N/A

Access=8021X , AuthMethod=EAP

Port Type=Wireless-802.11, Port Name=WLAN-DBSS1:0

Initial VLAN=200, Authorization VLAN=N/A

ACL Group=3000

User Profile=N/A

CAR=Disable

Traffic Statistic:

InputOctets =0 OutputOctets =0

InputGigawords=0 OutputGigawords=0

Priority=Disable

SessionTimeout=N/A, Terminate-Action=N/A

Start=2013-11-20 19:34:23 ,Current=2013-11-20 19:34:38 ,Online=00h00m15s

Total 1 connection matched.

- (3) Client 认证成功并获取 IP 地址后，能 ping 通 8.125.0.0/16 网段，无法 ping 通其他网段，证明授权 ACL 已生效。

```
C:\Documents and Settings\Administrator>ping 8.125.1.1
```

Pinging 8.125.1.1 with 32 bytes of data:

Reply from 8.125.1.1: bytes=32 time=6ms TTL=254

Reply from 8.125.1.1: bytes=32 time=12ms TTL=254

Reply from 8.125.1.1: bytes=32 time=46ms TTL=254

Reply from 8.125.1.1: bytes=32 time=25ms TTL=254

Ping statistics for 8.125.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 6ms, Maximum = 46ms, Average = 22ms

```
C:\Documents and Settings\Administrator>ping 125.100.1.1
```

Pinging 125.100.1.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 125.100.1.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

(4) 通过 **display acl** 命令可以查看到 ACL 3000 规则的匹配数量（略）。

## 4.6 配置文件

- AC:

```
#
port-security enable
#
dot1x authentication-method eap
#
acl number 3000
rule 0 permit ip destination 8.125.0.0 0.0.255.255
rule 1 deny ip
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
server-type extended
primary authentication 8.125.1.1
primary accounting 8.125.1.1
key authentication cipher $c$3$EnNB6wxpjYSAJMiU2aaeNArZaBzSA13G5A==
key accounting cipher $c$3$o9Wa5f+anDJ56GonM91E7c8otvLF06HKGA==
user-name-format without-domain
nas-ip 125.100.1.4
#
domain office
authentication lan-access radius-scheme office
authorization lan-access radius-scheme office
accounting lan-access none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 1
cipher-suite ccmp
security-ie rsn
service-template enable
```

```

#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200 300
#
interface Vlan-interface100
 ip address 125.100.1.4 255.255.0.0
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain office
 undo dot1x multicast-trigger
#
wlan ap officeap model WA2620E-AGN id 1
 serial-id 21023529G007C000020
 radio 1
 radio 2
 service-template 1 vlan-id 300
 radio enable
#
ip route-static 0.0.0.0 0.0.0.0 125.100.1.1
#

```

- **Switch:**

```

#
 dhcp enable
#
vlan 100
#
vlan 300
#
dhcp server ip-pool vlan100 extended
 network ip range 125.30.0.2 125.30.0.5
 network mask 255.255.0.0
 gateway-list 125.30.0.6
#
dhcp server ip-pool vlan300 extended
 network ip range 125.30.0.2 125.30.0.5
 network mask 255.255.0.0
 gateway-list 125.30.0.6
#
interface GigabitEthernet1/0/1

```



```
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
poe enable
#
```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“ACL 和 QoS 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“ACL 和 QoS 命令参考”。

# AC 1+1 热备份典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |    |
|------------------------|----|
| 1 简介.....              | 1  |
| 2 配置前提 .....           | 1  |
| 3 配置举例 .....           | 1  |
| 3.1 组网需求 .....         | 1  |
| 3.2 配置思路 .....         | 2  |
| 3.3 配置注意事项 .....       | 2  |
| 3.4 配置步骤 .....         | 2  |
| 3.4.1 AC 1 的配置 .....   | 2  |
| 3.4.2 AC 2 的配置 .....   | 3  |
| 3.4.3 Switch 的配置 ..... | 5  |
| 3.5 验证配置 .....         | 5  |
| 3.6 配置文件 .....         | 8  |
| 4 相关资料 .....           | 11 |

# 1 简介

本文档介绍 AC 1+1 热备份配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AC 1+1 热备份特性。

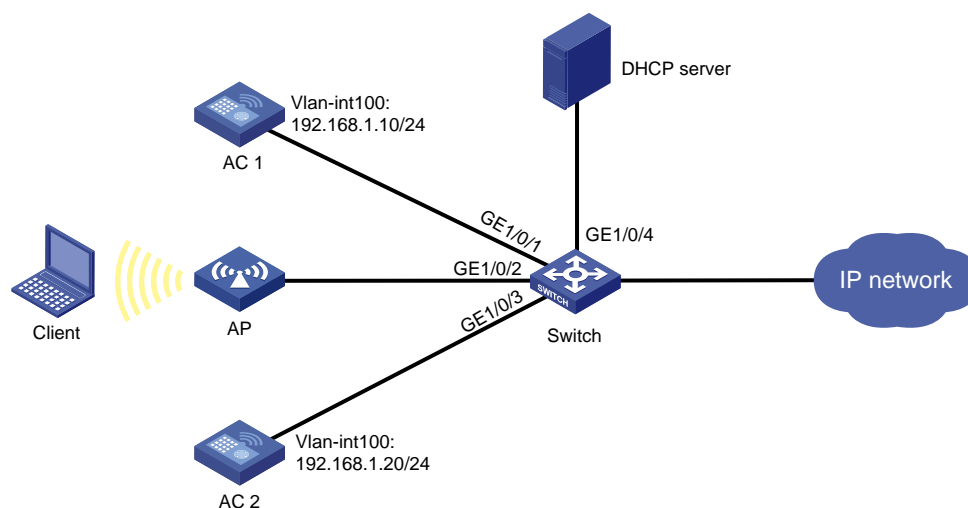
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，为了避免单台 AC 故障导致无线客户端无法接入网络，在网络中部署了两台 AC，实现 1+1 热备份。AC 1 作为主用 AC 负责提供无线服务，AC 2 作为备用 AC 为 AC1 提供备份，AC 1 与 AC 2 通过一台二层交换机相连。具体应用需求如下：

- AP 和 Client 通过 DHCP 服务器获取 IP 地址。
- 当 AC 1 发生故障时，能够立即切换到 AC 2 继续为 Client 提供无线服务；在 AC 1 故障恢复后，能够切换回 AC 1 为 Client 提供无线服务。

图1 AC 1+1 热备份组网图



## 3.2 配置思路

为了在主 AC 故障恢复后，AP 可以重新切换到主 AC 上，需要保证 AC 1 的优先级高于 AC 2。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 主、备 AC 上对于需要服务的同一 AP，其 AP 模板视图下的配置必须保持一致（除了 AC 的 IP 地址和优先级配置之外）。否则当 AC 的主、备状态切换之后，无法保证 AP 设备工作正常。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

(1) 配置 AC 1 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 192.168.1.10 255.255.255.0
[AC1-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 192.168.2.10 255.255.255.0
[AC1-Vlan-interface200] quit
```

# 在 AC 1 上配置热备份功能，同时配置 VLAN 200 作为 AC 间用于热备份的本端数据端口的 VLAN。

```
[AC1] hot-backup enable domain 1
[AC1] hot-backup vlan 200
```

# 在 AC 1 上配置 AC 2 的 IP 地址 192.168.1.20 为备份 AC 和 AP 建立隧道的接口的 IP 地址。

```
[AC1] wlan backup-ac ip 192.168.1.20
```

# 创建 WLAN-ESS 1 接口。

```
[AC1] interface wlan-ess 1
```

# 配置 WLAN-ESS 1 接口类型为 Hybrid。

```
[AC1-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。

```
[AC1-WLAN-ESS1] undo port hybrid vlan 1
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC1-WLAN-ESS1] mac-vlan enable
[AC1-WLAN-ESS1] quit
```

# 配置 AC 的 GigabitEthernet 1/0/1 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 200 通过。

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC1-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC1-GigabitEthernet1/0/1] quit
```

## (2) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC1] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC1-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC1-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
```

# 在 AC 1 的 AP 模板视图下配置 AP 名称为 officeap1，型号名称选择 WA2620E-AGN。

```
[AC1] wlan ap officeap1 model WA2620E-AGN
```

# 设置主 AC 上 AP 的接入优先级为 6，序列号为 21023529G007C000020。

```
[AC1-wlan-ap-officeap1] priority level 6
[AC1-wlan-ap-officeap1] serial-id 21023529G007C000020
```

# 进入 AP 的 radio1 射频视图，配置服务模板 1 与射频 1 进行关联，使能 AP 的 radio1 射频。

```
[AC1-wlan-ap-officeap1] radio 1
[AC1-wlan-ap-officeap1-radio-1] service-template 1
[AC1-wlan-ap-officeap1-radio-1] radio enable
[AC1-wlan-ap-officeap1-radio-1] quit
[AC1-wlan-ap-officeap1] quit
```

## 3.4.2 AC 2 的配置

### (1) 配置 AC 2 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 192.168.1.20 255.255.255.0
[AC2-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```

[AC2] vlan 200
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 192.168.2.20 255.255.255.0
[AC2-Vlan-interface200] quit
# 在 AC 2 上配置 hot-backup, 同时配置 VLAN 200 作为 AC 间用于热备份的本端数据端口的 VLAN。
[AC2] hot-backup enable domain 1
[AC2] hot-backup vlan 200
# 在 AC 2 上配置 AC 1 的 IP 地址 192.168.1.10 为主 AC 和 AP 建立隧道的接口的 IP 地址。
[AC2] wlan backup-ac ip 192.168.1.10
# 创建 WLAN-ESS 1 接口。
[AC2] interface wlan-ess 1
# 配置 WLAN-ESS 1 接口类型为 Hybrid。
[AC2-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200, 禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。
[AC2-WLAN-ESS1] undo port hybrid vlan 1
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
# 使能 MAC VLAN 功能。
[AC2-WLAN-ESS1] mac-vlan enable
[AC2-WLAN-ESS1] quit
# 配置 AC 的 GigabitEthernet 1/0/1 接口的链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 200 通过。
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC2-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC2-GigabitEthernet1/0/1] quit
(2) 配置无线服务
# 创建 clear 类型的服务模板 1。
[AC2] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service。
[AC2-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC2-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
# 在 AC 2 的 AP 模板视图下配置 AP 名称为 officeap1, 型号名称选择 WA2620E-AGN。
[AC2] wlan ap officeap1 model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020, 以及 AP 的接入优先级取系统缺省值 4。
[AC2-wlan-ap-officeap1] serial-id 21023529G007C000020
# 进入 AP 的 radio1 射频视图, 配置服务模板与射频 1 进行关联, 使能 AP 的 radio 1 射频。
[AC2-wlan-ap-officeap1] radio 1

```

```
[AC2-wlan-ap-officeap1-radio-1] service-template 1
[AC2-wlan-ap-officeap1-radio-1] radio enable
[AC2-wlan-ap-officeap1-radio-1] quit
[AC2-wlan-ap-officeap1] quit
```

### 3.4.3 Switch 的配置

# 创建 VLAN 100 和 VLAN 200, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 1 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 并允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access, 当前 Access 口允许 VLAN 100 通过, 并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AC 2 相连的 GigabitEthernet1/0/3 接口的链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 并允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type trunk
[Switch-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/3] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/4 接口的链路类型为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

## 3.5 验证配置

(1) 在主、备 AC 均正常工作时, 查看 AC 热备份状态、AP 运行状态和客户端运行状态。



# 在 AC 1 上通过命令行 **display hot-backup state** 查看 Link State 为 Connect、Peer Board MAC 为对端备份 AC 的 MAC 地址，Peer Board State 为 normal。

```
[AC1] display hot-backup state
*****
Vlan ID           : 20
Domain ID         : 1
Link State        : Connect
Peer Board MAC    : 000f-e27e-0bc7
Peer Board State  : Normal
Hello Interval    : 30
```

# 在 AC 2 上通过命令行 **display hot-backup state** 查看 Link State 为 Connect、Peer Board MAC 为对端主 AC 的 MAC 地址，Peer Board State 为 normal。

```
[AC2] display hot-backup state
*****
Vlan ID           : 20
Domain ID         : 1
Link State        : Connect
Peer Board MAC    : 000f-e212-ff01
Peer Board State  : Normal
Hello Interval    : 30
```

# 在 AC 1 上通过命令行 **display wlan ap** 查看 AP 的注册状态应该为 Run/M。

```
[AC1] display wlan ap name officeap1
                        AP Profile
-----
AP Name      APID State   Model      Serial-ID
-----
officeap1    1   Run/M    WA2620E-AGN  21023529G007C000020
-----
```

# 在 AC 2 上通过命令行 **display wlan ap** 查看 AP 的注册状态应该为 Run/B。

```
[AC2] display wlan ap name officeap1
                        AP Profile
-----
AP Name      APID State   Model      Serial-ID
-----
officeap1    1   Run/B    WA2620E-AGN  21023529G007C000020
-----
```

# 在 AC 1 上通过 **display wlan client** 命令可以看到上线的无线客户端状态为 Running。

```
[AC1] display wlan client
Total Number of Clients      : 1
Total Number of Clients Connected : 1
                        Client Information
-----
MAC Address      BSSID           AID   State      PS Mode  QoS Mode
-----
001b-110b-7274   000f-e28b-fd40    1     Running    Active   None
-----
```

# 在 AC 2 上通过 **display wlan client** 命令可以看到上线的无线客户端状态为 Running/B。

```
[AC2] display wlan client
```

```
Total Number of Clients          : 1
Total Number of Clients Connected : 1
```

Client Information

| MAC Address    | BSSID          | AID | State     | PS Mode | QoS Mode |
|----------------|----------------|-----|-----------|---------|----------|
| 001b-110b-7274 | 000f-e28b-fd40 | 1   | Running/B | Active  | None     |

(2) 当主 AC 发生故障和故障恢复时，查看 AP 状态与客户端状态的变化。

# 当 AC 1 发生故障时，本地 AP 连接的状态由 Run/B 切换为 Run/M，上线的无线客户端状态由 Running/B 变为 Running。

```
[AC2] display wlan ap name officeap1
```

AP Profile

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Run/M | WA2620E-AGN | 21023529G007C000020 |

```
[AC2] display wlan client
```

```
Total Number of Clients          : 1
Total Number of Clients Connected : 1
```

Client Information

| MAC Address    | BSSID          | AID | State   | PS Mode | QoS Mode |
|----------------|----------------|-----|---------|---------|----------|
| 001b-110b-7274 | 000f-e28b-fd40 | 1   | Running | Active  | None     |

# 在 AC 1 上通过 **display wlan ap** 命令查看 AP 的连接状态由 Run/M 切换为 Run/B，通过 **display wlan client** 命令可以看到上线的无线客户端状态为 Running/B。

```
[AC1] display wlan ap name officeap1
```

AP Profile

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Run/B | WA2620E-AGN | 21023529G007C000020 |

```
[AC1] display wlan client
```

```
Total Number of Clients          : 1
Total Number of Clients Connected : 1
```

Client Information

| MAC Address    | BSSID          | AID | State     | PS Mode | QoS Mode |
|----------------|----------------|-----|-----------|---------|----------|
| 001b-110b-7274 | 000f-e28b-fd40 | 1   | Running/B | Active  | None     |

# 当 AC 1 故障恢复后，在 AC 1 上通过 **display wlan ap** 命令查看 AP 的连接状态由 Run/B 切换为 Run/M，通过 **display wlan client** 命令可以看到上线的无线客户端状态为 Running。

```
[AC1] display wlan ap name officeap1
```

AP Profile

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Run/M | WA2620E-AGN | 21023529G007C000020 |

```
[AC1] display wlan client
```

Total Number of Clients : 1

Total Number of Clients Connected : 1

Client Information

| MAC Address    | BSSID          | AID | State   | PS Mode | QoS Mode |
|----------------|----------------|-----|---------|---------|----------|
| 001b-110b-7274 | 000f-e28b-fd40 | 1   | Running | Active  | None     |

# 在 AC 2 上通过 **display wlan ap** 命令查看 AP 的连接状态为 Run/B，通过 **display wlan client** 命令可以看到上线的无线客户端状态为 Running/B。

```
[AC2] display wlan ap name officeap1
```

AP Profile

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Run/B | WA2620E-AGN | 21023529G007C000020 |

```
[AC2] display wlan client
```

Total Number of Clients : 1

Total Number of Clients Connected : 1

Client Information

| MAC Address    | BSSID          | AID | State     | PS Mode | QoS Mode |
|----------------|----------------|-----|-----------|---------|----------|
| 001b-110b-7274 | 000f-e28b-fd40 | 1   | Running/B | Active  | None     |

## 3.6 配置文件

- AC 1:

```
#
wlan backup-ac ip 10.101.0.20
#
hot-backup enable domain 1
hot-backup vlan 200
#
```

```

vlan 100
#
vlan 200
#
wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable
#
interface Vlan-interface100
  ip address 192.168.1.10 255.255.255.0
#
interface Vlan-interface200
  ip address 192.168.2.10 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200
  port trunk pvid vlan 100
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
#
wlan ap officeap1 model WA2620E-AGN
  priority level 6
  serial-id 21023529G007C000020
  radio 1
    channel auto
    max-power 20
    service-template 1
    radio enable
#

```

- AC 2:

```

#
wlan backup-ac ip 10.101.0.10
#
  hot-backup enable domain 1
  hot-backup vlan 200
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
  ssid service

```

```

bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 192.168.1.20 255.255.255.0
#
interface Vlan-interface200
ip address 192.168.2.20 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
port hybrid vlan 1 200 untagged
#
wlan ap officeap1 model WA2620E-AGN
serial-id 21023529G007C000020
radio 1
channel auto
max-power 20
service-template 1
radio enable

```

#

- **Switch:**

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 100
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/4

```

```
port link-type access
port access vlan 100
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# AC 1+N 备份典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                          |    |
|--------------------------|----|
| 1 简介.....                | 1  |
| 2 配置前提 .....             | 1  |
| 3 配置举例 .....             | 1  |
| 3.1 组网需求 .....           | 1  |
| 3.2 配置思路 .....           | 2  |
| 3.3 注意事项 .....           | 2  |
| 3.4 配置步骤 .....           | 2  |
| 3.4.1 AC 1 的配置 .....     | 2  |
| 3.4.2 AC 2 的配置 .....     | 3  |
| 3.4.3 BackupAC 的配置 ..... | 5  |
| 3.4.4 Switch 的配置 .....   | 6  |
| 3.5 验证配置 .....           | 7  |
| 3.6 配置文件 .....           | 9  |
| 4 相关资料 .....             | 12 |



# 1 简介

本文档介绍了 AC 1+N 备份配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AC 1+N 备份特性。

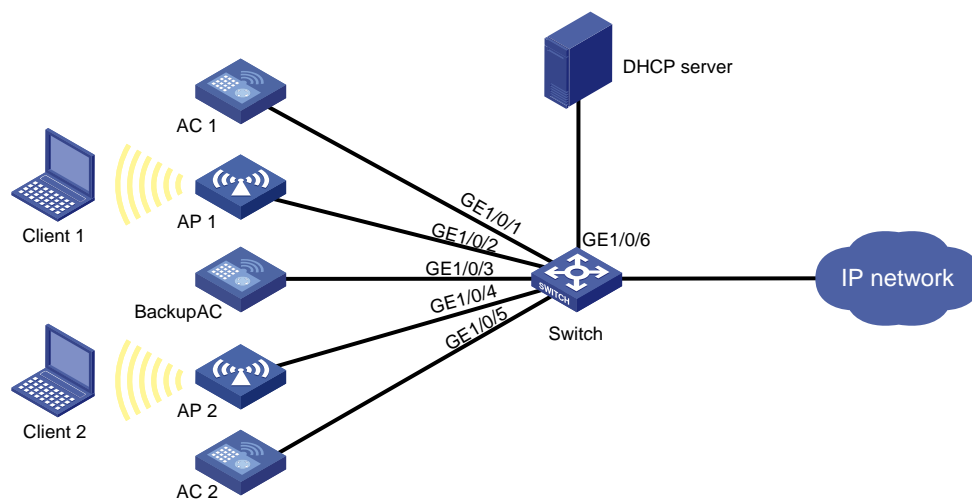
## 3 配置举例

### 3.1 组网需求

如图 1 所示，无线网络中有两台无线控制器 AC 1 和 AC 2，分别为 AP 1 和 AP 2 提供无线服务。现要求在网络中增加一台 AC，作为两台主 AC 的备份 AC，具体应用需求如下：

- 在检测到主 AC 故障后的 30 秒内，AP 会主动切换连接到备份 AC 上。
- 当主 AC 故障恢复后，AP 会尝试去和主 AC 重新协商并建立隧道，如果建立成功，则 AP 会切断和备份 AC 的连接，自动切换到主 AC 上。

图1 1+N 备份组网图



## 3.2 配置思路

- 为了实现 AC 间的主备切换，当主 AC 故障时，AP 需要获取备份 AC 的 IP 地址，所以需要在 BackupAC 的 AP 1 和 AP 2 模板视图下分别配置 AC 1 和 AC 2 的 IP 地址。
- 为了可以在主 AC 故障恢复后，AP 可以重新切换到主 AC 上，需要保证在 AC 1 和 AC 2 上配置的接入优先级都高于 BackupAC 上配置的接入优先级。

## 3.3 注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 主、备 AC 的软件版本需要保持一致。
- 主、备 AC 上对于需要提供服务的同一 AP，其 AP 模板视图下的配置必须保持一致（除了 AC 的 IP 地址和优先级配置之外）。否则当 AC 的主、备状态切换之后，无法保证 AP 设备工作正常。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

#### (1) 配置 AC 1 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 1 将使用该接口的 IP 地址与 AP 1 建立 LWAPP 隧道。

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 10.101.0.10 255.255.255.0
[AC1-Vlan-interface100] quit
```

# 创建 VLAN 200，作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 10.101.1.10 255.255.255.0
[AC1-Vlan-interface200] quit
```

# 创建 WLAN-ESS 1 接口。

```
[AC1] interface wlan-ess 1
```

# 配置 WLAN-ESS 1 接口的链路类型为 Hybrid。

```
[AC1-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，并允许 VLAN 200 不带 Tag 通过。

```
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC1-WLAN-ESS1] mac-vlan enable
```

```
[AC1-WLAN-ESS1] quit
```

# 配置 AC 的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，允许 VLAN 100 和 VLAN 200 的报文通过。

```
[AC1] interface gigabitethernet 1/0/1
```

```
[AC1-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[AC1-GigabitEthernet1/0/1] quit
```

## (2) 配置服务模板

# 创建 clear 类型的服务模板 1。

```
[AC1] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 TC。

```
[AC1-wlan-st-1] ssid TC
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC1-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC1-wlan-st-1] service-template enable
```

```
[AC1-wlan-st-1] quit
```

## (3) 配置 AP

# 在主 AC 1 的 AP 模板视图下配置 AP 1 的名称为 officeap1，型号为 WA2620E-AGN。

```
[AC1] wlan ap officeap1 model WA2620E-AGN
```

# 设置 AC 1 上 AP 1 的接入优先级为 7，序列号为 21023529G007C000020。

```
[AC1-wlan-ap-officeap1] priority level 7
```

```
[AC1-wlan-ap-officeap1] serial-id 21023529G007C000020
```

# 进入 AP 1 的 radio1 射频视图，配置服务模板与射频 1 进行关联，使能 AP 1 的 radio1 射频。

```
[AC1-wlan-ap-officeap1] radio 1
```

```
[AC1-wlan-ap-officeap1-radio-1] service-template 1
```

```
[AC1-wlan-ap-officeap1-radio-1] radio enable
```

```
[AC1-wlan-ap-officeap1-radio-1] quit
```

```
[AC1-wlan-ap-officeap1] quit
```

## 3.4.2 AC 2 的配置

### (1) 配置 AC 2 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 2 将使用该接口的 IP 地址与 AP 2 建立 LWAPP 隧道。

```
<AC2> system-view
```

```
[AC2] vlan 100
```

```
[AC2-vlan100] quit
```

```
[AC2] interface vlan-interface 100
```

```
[AC2-Vlan-interface100] ip address 10.101.0.30 255.255.255.0
```

```
[AC2-Vlan-interface100] quit
```

# 创建 VLAN 200，作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC2] vlan 200
```

```

[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 10.101.1.30 255.255.255.0
[AC2-Vlan-interface200] quit
# 创建 WLAN-ESS 1 接口。
[AC2] interface wlan-ess 1
# 配置 WLAN-ESS 1 接口的链路类型为 Hybrid。
[AC2-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，并允许 VLAN 200 不带 Tag 通过。
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
# 使能 MAC VLAN 功能。
[AC2-WLAN-ESS1] mac-vlan enable
[AC2-WLAN-ESS1] quit
# 配置 AC 的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，允许 VLAN 100 和 VLAN 200 的报文通过。
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC2-GigabitEthernet1/0/1] quit
(2) 配置服务模板
# 创建 clear 类型的服务模板 1。
[AC2] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 TC。
[AC2-wlan-st-1] ssid TC
# 将 WLAN-ESS 1 接口绑定到服务模板 1。
[AC2-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
(3) 配置 AP
# 在主 AC 2 的 AP 模板视图下配置 AP 2 的名称为 officeap2，型号为 WA2620E-AGN。
[AC2] wlan ap officeap2 model WA2620E-AGN
# 设置 AC 2 上 AP 2 的接入优先级为 7，序列号为 21023529G007C000021
[AC2-wlan-ap-officeap2] priority level 7
[AC2-wlan-ap-officeap2] serial-id 21023529G007C000021
# 进入 AP 2 的 radio1 射频视图，配置服务模板与射频 1 进行关联，使能 AP 2 的 radio1 射频。
[AC2-wlan-ap-officeap2] radio 1
[AC2-wlan-ap-officeap2-radio-1] service-template 1
[AC2-wlan-ap-officeap2-radio-1] radio enable
[AC2-wlan-ap-officeap2-radio-1] quit
[AC2-wlan-ap-officeap2] quit

```

### 3.4.3 BackupAC 的配置

#### (1) 配置 BackupAC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。BackupAC 将使用该接口的 IP 地址与 AP 1 和 AP 2 建立 LWAPP 隧道。

```
<BackupAC> system-view
[BackupAC] vlan 100
[BackupAC-vlan100] quit
[BackupAC] interface vlan-interface 100
[BackupAC-Vlan-interface100] ip address 10.101.0.20 255.255.255.0
[BackupAC-Vlan-interface100] quit
```

# 创建 VLAN 200，作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[BackupAC] vlan 200
[BackupAC-vlan200] quit
[BackupAC] interface vlan-interface 200
[BackupAC-Vlan-interface200] ip address 10.101.1.20 255.255.255.0
[BackupAC-Vlan-interface200] quit
```

# 创建 WLAN-ESS 1 接口。

```
[BackupAC] interface wlan-ess 1
```

# 配置 WLAN-ESS 1 接口的链路类型为 Hybrid。

```
[BackupAC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，并允许 VLAN 200 不带 Tag 通过。

```
[BackupAC-WLAN-ESS1] port hybrid vlan 200 untagged
[BackupAC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[BackupAC-WLAN-ESS1] mac-vlan enable
[BackupAC-WLAN-ESS1] quit
```

# 配置 BackupAC 的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，允许 VLAN 100 和 VLAN 200 的报文通过。

```
[BackupAC] interface gigabitethernet 1/0/1
[BackupAC-GigabitEthernet1/0/1] port link-type trunk
[BackupAC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[BackupAC-GigabitEthernet1/0/1] quit
```

#### (2) 配置服务模板

# 创建 clear 类型的服务模板 1。

```
[BackupAC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 TC。

```
[BackupAC-wlan-st-1] ssid TC
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[BackupAC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[BackupAC-wlan-st-1] service-template enable
[BackupAC-wlan-st-1] quit
```

#### (3) 配置 AP

# 在 BackupAC 的对应 AP 1 视图下配置 AP 1 名称为 officeap1，型号为 WA2620E-AGN，序列号为 21023529G007C000020，AP 1 的接入优先级取系统缺省值 4。

```
[BackupAC] wlan ap officeap1 model WA2620E-AGN
[BackupAC-wlan-ap-officeap1] serial-id 21023529G007C000020
```

# 在 BackupAC 的 AP 1 模板视图下，配置 AC 1 的 IP 地址。

```
[BackupAC-wlan-ap-officeap1] backup-ac ip 10.101.0.10
```

# 进入 AP 1 的 radio1 射频视图，将服务模板与射频 1 进行关联，并使能 AP 1 的 radio1 射频。

```
[BackupAC-wlan-ap-officeap1] radio 1
[BackupAC-wlan-ap-officeap1-radio-1] service-template 1
[BackupAC-wlan-ap-officeap1-radio-1] radio enable
[BackupAC-wlan-ap-officeap1-radio-1] quit
[BackupAC-wlan-ap-officeap1] quit
```

# 在 BackupAC 的对应 AP 2 视图下配置 AP 2 名称为 officeap2，型号为 WA2620E-AGN，序列号为 21023529G007C000021，AP 2 的接入优先级取系统缺省值 4。

```
[BackupAC] wlan ap officeap2 model WA2620E-AGN
[BackupAC-wlan-ap-officeap2] serial-id 21023529G007C000021
```

# 在 BackupAC 的 AP 2 模板视图下，配置 AC 2 的 IP 地址。

```
[BackupAC-wlan-ap-officeap2] backup-ac ip 10.101.0.30
```

# 进入 AP 2 的 radio1 射频视图，将服务模板与射频 1 进行关联，并使能 AP 2 的 radio1 射频。

```
[BackupAC-wlan-ap-officeap2] radio 1
[BackupAC-wlan-ap-officeap2-radio-1] service-template 1
[BackupAC-wlan-ap-officeap2-radio-1] radio enable
[BackupAC-wlan-ap-officeap2-radio-1] quit
[BackupAC-wlan-ap-officeap2] return
```

### 3.4.4 Switch 的配置

# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 1 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 200 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口链路类型为 Access，当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 BackupAC 相连的 GigabitEthernet1/0/3 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 200 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type trunk
[Switch-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/3] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/4 接口链路类型为 Access，当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

# 配置 Switch 与 AC 2 相连的 GigabitEthernet1/0/5 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 200 通过。

```
[Switch] interface gigabitethernet 1/0/5
[Switch-GigabitEthernet1/0/5] port link-type trunk
[Switch-GigabitEthernet1/0/5] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/5] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/5] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/6 接口链路类型为 Access，当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/6
[Switch-GigabitEthernet1/0/6] port link-type access
[Switch-GigabitEthernet1/0/6] port access vlan 100
[Switch-GigabitEthernet1/0/6] quit
```

### 3.5 验证配置

(1) 在 AC 1 上通过命令行 **display wlan ap name officeap1** 查看 AP 1 的注册状态为 Run/M。

```
<AC1> display wlan ap name officeap1
```

AP Profile

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Run/M | WA2620E-AGN | 21023529G007C000020 |

(2) 在备份 AC 上通过命令行 **display wlan ap name officeap1** 查看 AP 1 的注册状态应该为 Idle。

```
<BackupAC> display wlan ap name officeap1
```

AP Profile

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Idle  | WA2620E-AGN | 21023529G007C000020 |

- (3) 通过命令行 **shutdown** 断开 AC 1 和 AP 1 的连接，待隧道超时后，在 AC 1 上使用 **display wlan ap name officeap1** 命令查看 AP 1 的注册状态应该为 Idle。

```
<AC1> system-view
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] shutdown
#Mar 31 15:03:53:315 2014 AC IFNET/4/INTERFACE UPDOWN:
  Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 20054116 is Down, ifAdminStatus is 2,
ifOperStatus is 2
%Mar 31 15:03:53:317 2014 AC IFNET/4/LINK UPDOWN:
  Vlan-interface100: link status is DOWN
%Mar 31 15:03:53:361 2014 AC IFNET/4/UPDOWN:
  Line protocol on the interface Vlan-interface100 is DOWN

[AC1-Vlan-interface100]
#Mar 31 15:04:21:587 2014 AC LWPS/4/Tunnel Down: Tunnel Down:1.3.6.1.4.1.
25506.2.75.1.3.0.2<hh3cDot11ACMtTunnelDownTrap> Serial Id:21023529G007C000020 DownInfo:1
#Mar 31 15:04:22:102 2014 AC IFNET/4/INTERFACE UPDOWN:
  Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 20905984 is Down, ifAdminStatus is 2,
ifOperStatus is 2
#Mar 31 15:04:22:107 2014 AC IFNET/4/INTERFACE UPDOWN:
  Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 20840448 is Down, ifAdminStatus is 1,
ifOperStatus is 2
%Mar 31 15:04:22:117 2014 AC IFNET/4/LINK UPDOWN:
  WLAN-DBSS1:19: link status is DOWN
%Mar 31 15:04:22:127 2014 AC IFNET/4/LINK UPDOWN:
  WLAN-ESS1: link status is DOWN

[AC1-Vlan-interface100] display wlan ap name officeap1
                        AP Profile
```

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Idle  | WA2620E-AGN | 21023529G007C000020 |

- (4) 在 BackupAC 上使用 **display wlan ap name officeap1** 命令查看 AP 1 的注册状态应该变为 Run/M。

```
#Mar 31 15:01:42:436 2014 BackupAC LWPS/4/Tunnel Up: Tunnel Up:1.3.6.1.4.1.2014
.10.2.75.1.3.0.1<h3cDot11ACMtTunnelSetupTrap> Serial Id:21023529G007C000020 UpInfo:1
<BackupAC> display wlan ap name officeap1
                        AP Profile
```

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Run/M | WA2620E-AGN | 21023529G007C000020 |

- (5) 使用 **undo shutdown** 命令关闭 AC 1 的 VLAN 接口 100，过一段时间后，在 AC 1 上可以看到 AC 1 和 AP 1 建立起隧道，通过 **display wlan ap name officeap1** 命令可以看到 AP 1 的注册状态为 Run/M。



```
[AC1-Vlan-interface100] undo shutdown
#Mar 31 15:11:10:610 2014 AC IFNET/4/INTERFACE UPDOWN:
  Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 20054116 is Up, ifAdminStatus is 1,
  ifOperStatus is 1
%Mar 31 15:11:10:656 2014 AC IFNET/4/LINK UPDOWN:
  Vlan-interface100: link status is UP
%Mar 31 15:11:10:657 2014 AC IFNET/4/UPDOWN:
  Line protocol on the interface Vlan-interface100 is UP
[AC1-Vlan-interface100]
#Mar 31 15:11:28:015 2014 AC LWPS/4/Tunnel Up: Tunnel Up:1.3.6.1.4.1.2550
6.2.75.1.3.0.1<hh3cDot11ACMtTunnelSetupTrap> Serial Id:21023529G007C000020 UpInfo:1
```

```
[AC1-Vlan-interface100] display wlan ap name officeap1
AP Profile
```

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Run/M | WA2620E-AGN | 21023529G007C000020 |

(6) 在 BackupAC 上使用 **display wlan ap name officeap1** 命令可以看到 AP 1 的注册状态变为 Idle。

```
<BackupAC> display wlan ap name officeap1
AP Profile
```

| AP Name   | APID | State | Model       | Serial-ID           |
|-----------|------|-------|-------------|---------------------|
| officeap1 | 1    | Idle  | WA2620E-AGN | 21023529G007C000020 |

## 3.6 配置文件

- AC 1:

```
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
  ssid TC
  bind WLAN-ESS 1
  service-template enable
#
interface Vlan-interface100
  ip address 10.101.0.10 255.255.255.0
#
interface Vlan-interface200
  ip address 10.101.1.10 255.255.255.0
#
```

```

interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 100 200
#
interface WLAN-ESS1
  port link-type hybrid
  port hybrid vlan 1 200 untagged
#
wlan ap officeap1 model WA2620E-AGN
  priority level 7
  serial-id 21023529G007C000020
  radio 1
    channel auto
    max-power 20
    service-template 1
    radio enable
#
•   AC 2:
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
  ssid TC
  bind WLAN-ESS 1
  service-template enable
#
interface Vlan-interface100
  ip address 10.101.0.30 255.255.255.0
#
interface Vlan-interface200
  ip address 10.101.1.30 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 100 200
#
interface WLAN-ESS1
  port link-type hybrid
  port hybrid vlan 1 200 untagged
#
wlan ap officeap2 model WA2620E-AGN
  priority level 7
  serial-id 21023529G007C000021
  radio 1

```

```

channel auto
max-power 20
service-template 1
radio enable
#
•   BackupAC:
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
ssid TC
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 10.101.0.20 255.255.255.0
#
interface Vlan-interface200
ip address 10.101.1.20 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 100 200
#
interface WLAN-ESS1
port link-type hybrid
port hybrid vlan 1 200 untagged
wlan ap officeap1 model WA2620E-AGN
serial-id 21023529G007C000020
backup-ac ip 10.101.0.10
radio 1
channel auto
max-power 20
service-template 1
radio enable
wlan ap officeap2 model WA2620E-AGN
serial-id 21023529G007C000021
backup-ac ip 10.101.0.30
radio 1
channel auto
max-power 20
service-template 1
radio enable
#
•   Switch:

```

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 100
#
interface GigabitEthernet1/0/3
    port link-type trunk
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/4
    port link-type trunk
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/5
    port link-type access
    port access vlan 100
#
interface GigabitEthernet1/0/6
    port link-type access
    port access vlan 100
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# AC 内二层漫游典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项.....        | 2 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 3 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 5 |
| 4 相关资料 .....           | 6 |

# 1 简介

本文档介绍无线客户端在属于同一 VLAN 的 AP 间进行二层漫游的典型配置案例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

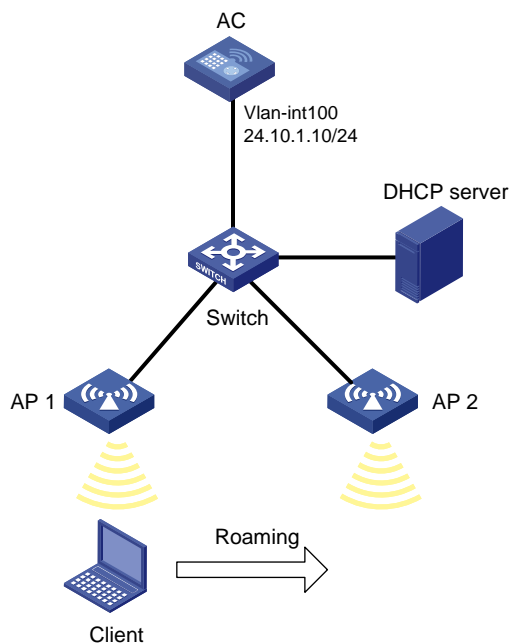
本文档假设您已了解 AAA、802.1X 和 WLAN 漫游特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC、AP 1 和 AP 2 在 VLAN 100 中，无线客户端先通过 AP 1 连接至无线网络，然后漫游到与同一 AC 相连的 AP 2 上。

图1 AC 内二层漫游组网图



### 3.2 配置思路

- 为了实现 AC 内漫游，各 AP 配置相同的 SSID，各 AP 下绑定相同的服务模板。

- 由于无线客户端在跨 VLAN 漫游过程中需要通过 MAC VLAN 表项强制保持自身的 VLAN 不变，所以需要开启 MAC-VLAN 功能。

### 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.4 配置步骤

#### 3.4.1 AC 的配置

##### (1) 配置 AC 的 IP 地址

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 24.10.1.10 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

##### (2) 配置无线接口

# 创建 WLAN-ESS1 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200, 禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 intra-roam。

```
[AC-wlan-st-1] ssid intra-roam
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 开启服务模板 1。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```



### (3) 配置射频接口并绑定服务模板

# 配置 AP 1: 创建 AP 1 的模板, 名称为 ap1, 型号名称选择 WA2620E-AGN, 并配置 AP 1 的序列号。

```
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 21023529G007C000020
[AC-wlan-ap-ap1] radio 2
```

# 将服务模板 1 绑定到 AP 1 的 radio 2 口。

```
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

# 配置 AP 2: 创建 AP 2 的模板, 名称为 ap2, 型号名称选择 WA2620E-AGN, 并配置 AP 2 的序列号。

```
[AC] wlan ap ap2 model WA2620E-AGN
[AC-wlan-ap-ap2] serial-id 21023529G007C000021
[AC-wlan-ap-ap2] radio 2
```

# 将服务模板 1 绑定到 AP 2 的 radio 2 口。

```
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2] quit
```

## 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 的 GigabitEthernet1/0/1 接口的属性为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 200 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

## 3.5 验证配置

# 漫游前在 AC 上使用命令 **display wlan client verbose** 查看显示信息如下:

```
[AC] display wlan client verbose
Total Number of Clients      : 1
                             Client Information
-----
MAC Address                  : 0037-6dec-7ea2
User Name                    : -NA-
IP Address                    : 21.10.1.4
AID                           : 1
AP Name                       : ap1
Radio Id                     : 2
Antenna Id                   : 0
Service Template Number      : 1
SSID                         : intra-roam
BSSID                        : 80f6-2ee1-48d0
Port                          : WLAN-DBSS1:28
VLAN                          : 100
State                         : Running
Power Save Mode               : Sleep
Wireless Mode                 : 11g
QoS Mode                      : WMM
Listen Interval (Beacon Interval) : 10
RSSI                          : 52
Rx/Tx Rate                   : 54/36
Client Type                   : PRE-RSNA
Authentication Method         : Open System
Authentication Mode           : Central
AKM Method                    : None
4-Way Handshake State         : -NA-
Group Key State               : -NA-
Encryption Cipher             : Clear
Roam Status                   : Normal
Roam Count                    : 0
Up Time (hh:mm:ss)           : 00:01:25
-----
```

# 漫游过程中在 AC 上看到如下信息:

```
Apr 17 10:59:52:341 2013 AC WROAM/6/WROAM_ROAM_HAPPEN: Client 0037-6de
c-7ea2 roamed from BSSID 80f6-2ee1-48d0 of AC 127.0.0.1 to BSSID 5866-ba94-71f0
of AC 127.0.0.1.
```

# 漫游完成后在 AC 上使用命令 **display wlan client verbose** 查看如下:

```
[AC] display wlan client verbose
Total Number of Clients      : 1
                             Client Information
```

```

-----
MAC Address           : 0037-6dec-7ea2
User Name             : -NA-
IP Address            : 21.10.1.4
AID                   : 1
AP Name               : ap2
Radio Id              : 2
Antenna Id            : 0
Service Template Number : 1
SSID                  : intra-roam
BSSID                 : 5866-ba94-71f0
Port                  : WLAN-DBSS1:25
VLAN                  : 100
State                 : Running
Power Save Mode        : Sleep
Wireless Mode         : 11g
QoS Mode              : WMM
Listen Interval (Beacon Interval) : 10
RSSI                  : 45
Rx/Tx Rate            : 54/0
Client Type           : PRE-RSNA
Authentication Method  : Open System
Authentication Mode    : Central
AKM Method             : None
4-Way Handshake State  : -NA-
Group Key State        : -NA-
Encryption Cipher      : Clear
Roam Status            : Intra-AC roam association
Roam Count             : 1
Up Time (hh:mm:ss)    : 00:00:11
-----

```

在漫游结束后，从以上显示信息可以查看到该客户端关联的 AP Name 由 ap1 变成了 ap2，漫游状态（Roam Status）为 Intra-AC roam association，漫游次数（Roam Count）为 1；说明客户端在 AC 内已经由 AP1 漫游到 AP2，成功漫游 1 次。

## 3.6 配置文件

- AC:

```

#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
ssid intra-roam
bind WLAN-ESS 1
service-template enable

```

```

#
interface Vlan-interface100
 ip address 24.10.1.10 255.255.255.0
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
 serial-id 21023529G007C000020
 radio 1
 radio 2
 service-template 1
 radio enable
#
wlan ap ap2 model WA2620E-AGN id 2
 serial-id 21023529G007C000021
 radio 1
 radio 2
 service-template 1
 radio enable
#
• Switch:
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# AC 内三层漫游典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                           |   |
|---------------------------|---|
| 1 简介.....                 | 1 |
| 2 配置前提 .....              | 1 |
| 3 配置举例 .....              | 1 |
| 3.1 组网需求 .....            | 1 |
| 3.2 配置思路 .....            | 2 |
| 3.3 配置注意事项.....           | 2 |
| 3.4 配置步骤 .....            | 2 |
| 3.4.1 AC 的配置 .....        | 2 |
| 3.4.2 L3 switch 的配置 ..... | 3 |
| 3.5 验证配置 .....            | 5 |
| 3.6 配置文件 .....            | 7 |
| 4 相关资料 .....              | 8 |

# 1 简介

本文档介绍 AC 内三层漫游的典型配置案例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

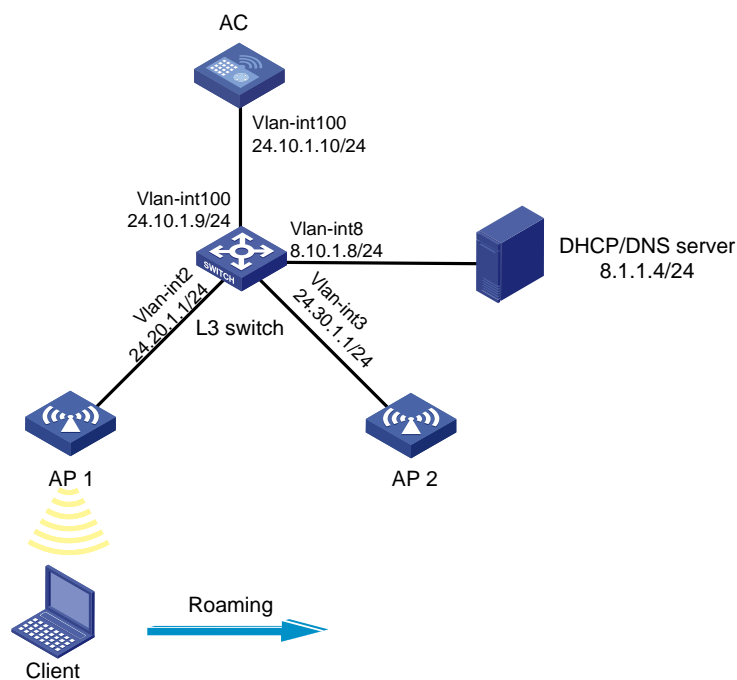
本文档假设您已了解 WLAN 漫游特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 在 VLAN 100 内，AP 1 在 VLAN 2 内，AP 2 在 VLAN 3 内，Client 和 AP 通过 DHCP server 获取 IP 地址。要求：无线客户端先通过 AP 1 连接至无线网络，然后漫游到与同一 AC 相连的 AP 2 上。

图1 AC 内三层漫游组网图



## 3.2 配置思路

- 为了实现 AC 内漫游，需要为各 AP 配置相同的 SSID，同时要为各 AP 绑定相同的服务模板。
- 由于无线客户端在跨 VLAN 漫游过程中需要通过 MAC VLAN 表项强制保持自身的 VLAN 不变，所以需要开启 MAC-VLAN 功能。

## 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 网络基本配置

# 配置 AC 的缺省路由。

```
<AC> system-view
[AC] ip route-static 0.0.0.0 0 24.10.1.9
```

#### (2) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。同时 VLAN 100 也作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 24.10.1.10 24
[AC-Vlan-interface100] quit
```

# 配置二层 GigabitEthernet1/0/1 接口以及其对应的成员端口的链路类型为 trunk，当前 trunk 口的 PVID 为 100，允许 VLAN 100（AC 和 AP 间建立 LWAPP 隧道的 VLAN）通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (3) 配置无线服务

# 创建接口 WLAN-ESS 1 并进入其视图。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 100，禁止 VLAN 1 通过并允许 VLAN 100 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid pvid vlan 100
[AC-WLAN-ESS1] port hybrid vlan 100 untagged
```

# 在 Hybrid 端口上使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```



```

# 创建 clear 类型的服务模板 1。
[AC] wlan service-template 1 clear
# 配置当前服务模板的 SSID 为 service1。
[AC-wlan-st-1] ssid service1
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 使能服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(4) 配置射频接口并绑定服务模板
# 在 AC 上配置 AP 名称为 ap1，型号名称选择 WA2620E-AGN，并配置序列号。
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 21023529G007C000020
# 配置 ap1 的 radio 2 的射频类型为 802.11gn。
[AC-wlan-ap-ap1] radio 2 type dot11gn
# 将服务模板 1 绑定到 AP 1 的 radio 2 口。
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
# 在 AC 上配置 AP 名称为 ap2，型号名称选择 WA2620E-AGN，并配置序列号。
[AC] wlan ap ap2 model WA2620E-AGN
[AC-wlan-ap-ap2] serial-id 21023529G007C000021
# 配置 ap2 的 radio 2 的射频类型为 802.11gn。
[AC-wlan-ap-ap2] radio 2 type dot11gn
# 将服务模板 1 绑定到 AP 2 的 radio 2 口。
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit

```

### 3.4.2 L3 switch 的配置

# 创建 VLAN 2、VLAN 3、VLAN 8 和 VLAN 100。其中 VLAN 2 用来接收 AP 1 的报文，VLAN 3 用来接收 AP 2 的报文，VLAN 8 用来接收 DHCP/DNS server 的报文，VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量。

```

<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] vlan 3
[Switch-vlan3] quit
[Switch] vlan 8
[Switch-vlan8] quit
[Switch] vlan 100
[Switch-vlan100] quit

```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Trunk，并允许 VLAN 2 和 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 2 100
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 2
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Trunk，并允许 VLAN 3 和 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type trunk
[Switch-GigabitEthernet1/0/3] port trunk permit vlan 3 100
[Switch-GigabitEthernet1/0/3] port trunk pvid vlan 3
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 DHCP/DNS server 相连的 GigabitEthernet1/0/4 接口属性为 Trunk，并允许 VLAN 8 和 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk permit vlan 8 100
[Switch-GigabitEthernet1/0/3] port trunk pvid vlan 8
[Switch-GigabitEthernet1/0/4] quit
```

# 配置各 VLAN 接口的 IP 地址。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 24.20.1.1 255.255.255.0
[Switch-Vlan-interface2] quit
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 24.30.1.1 255.255.255.0
[Switch-Vlan-interface3] quit
[Switch] interface vlan-interface 8
[Switch-Vlan-interface8] ip address 8.10.1.8 255.255.255.0
[Switch-Vlan-interface8] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 24.10.1.10 255.255.255.0
[Switch-Vlan-interface100] quit
```

## 3.5 验证配置

# 使用命令 **display wlan ap all** 显示 AP 状态，都处于 running:

```
[AC] display wlan ap all
Total Number of APs configured          : 2
Total Number of configured APs connected : 2
Total Number of auto APs connected      : 0

AP Profiles
State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
       C = Config, R = Run, KU = KeyUpdate, KC = KeyCfm
```

| AP Name | State | Model       | Serial-ID           |
|---------|-------|-------------|---------------------|
| ap1     | R/M   | WA2620E-AGN | 21023529G007C000020 |
| ap2     | R/M   | WA2620E-AGN | 21023529G007C000021 |

# 从下面显示可以看出，Client 漫游前在 AP1 上。

```
[AC] display wlan client verbose
Total Number of Clients          : 1

Client Information

MAC Address                      : 0021-631e-7911
User Name                       : -NA-
AID                             : 1
AP Name                         : ap1
Radio Id                       : 2
SSID                           : service1
BSSID                           : 5866-ba28-2b70
Port                           : WLAN-DBSS5:18
VLAN                           : 100
State                           : Running
Power Save Mode                 : Active
Wireless Mode                   : 11gn
Channel Band-width              : 20MHz
SM Power Save Enable            : Disabled
Short GI for 20MHz               : Not Supported
Short GI for 40MHz              : Not Supported
Support MCS Set                  : 0,1,2,3,4,5,6,7,8,9,
                                10,11,12,13,14,15
BLOCK ACK-TID 0                 : IN
QoS Mode                        : WMM
Listen Interval (Beacon Interval) : 10
RSSI                            : 55
Rx/Tx Rate                      : 104/130
Client Type                     : PRE-RSNA
Authentication Method            : Open System
Authentication Mode              : Central
AKM Method                      : None
```

```

4-Way Handshake State      : -NA-
Group Key State            : -NA-
Encryption Cipher          : Clear
Roam Status                : Normal
Roam Count                 : 0
Up Time (hh:mm:ss)        : 00:11:55

```

---

# 从以下显示信息可以看出，Client 漫游到了 AP2 上。

```
[AC] display wlan client verbose
```

```

Total Number of Clients      : 1
                          Client Information

```

---

```

MAC Address                 : 0021-631e-7911
User Name                   : -NA-
AID                         : 1
AP Name                     : ap2
Radio Id                    : 2
SSID                        : service1
BSSID                       : 80f6-2eba-3320
Port                        : WLAN-DBSS5:18
VLAN                        : 100
State                       : Running
Power Save Mode             : Active
Wireless Mode               : 11gn
Channel Band-width         : 20MHz
SM Power Save Enable        : Disabled
Short GI for 20MHz          : Not Supported
Short GI for 40MHz          : Not Supported
Support MCS Set              : 0,1,2,3,4,5,6,7,8,9,
                              10,11,12,13,14,15
BLOCK ACK-TID 0             : IN
QoS Mode                    : WMM
Listen Interval (Beacon Interval) : 10
RSSI                        : 55
Rx/Tx Rate                  : 104/130
Client Type                  : PRE-RSNA
Authentication Method        : Open System
Authentication Mode          : Central
AKM Method                   : None
4-Way Handshake State       : -NA-
Group Key State              : -NA-
Encryption Cipher            : Clear
Roam Status                  : Intra-AC roam association
Roam Count                   : 1
Up Time (hh:mm:ss)          : 00:11:55

```

---

## 3.6 配置文件

- AC:

```
#
vlan 100
#
wlan service-template 1 clear
  ssid servicel
  bind WLAN-ESS 1
  service-template enable
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100
#
interface Vlan-interface100
  ip address 24.10.1.10 255.255.255.0
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 100 untagged
  port hybrid pvid vlan 100
  mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
    service-template 1
  radio enable
#
wlan ap ap2 model WA2620E-AGN id 2
  serial-id 21023529G007C000021
  radio 1
  radio 2
    service-template 1
  radio enable
#
ip route-static 0.0.0.0 0.0.0.0 24.10.1.9
#
```

- L3 switch:

```
#
vlan 2 to 3
#
vlan 8
#
vlan 100
```

```

#
interface Vlan-interface2
 ip address 24.20.1.1 255.255.255.0
#
interface Vlan-interface3
 ip address 24.30.1.1 255.255.255.0
#
interface Vlan-interface8
 ip address 8.10.1.8 255.255.255.0
#
interface Vlan-interface100
 ip address 24.10.1.10 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 100
 port trunk pvid vlan 2
 poe enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3 100
 port trunk pvid vlan 3
 poe enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 8 100
 port trunk pvid vlan 8
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 客户端在 AC 间漫游典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                            |    |
|----------------------------|----|
| 1 简介.....                  | 1  |
| 2 配置前提 .....               | 1  |
| 3 配置举例 .....               | 1  |
| 3.1 组网需求 .....             | 1  |
| 3.2 配置思路 .....             | 2  |
| 3.3 配置注意事项 .....           | 2  |
| 3.4 配置步骤 .....             | 2  |
| 3.4.1 AC 1 的配置 .....       | 2  |
| 3.4.2 AC 2 的配置 .....       | 4  |
| 3.4.3 L3 switch 的配置 .....  | 7  |
| 3.4.4 AAA server 的配置 ..... | 8  |
| 3.5 验证配置 .....             | 10 |
| 3.6 配置文件 .....             | 12 |
| 4 相关资料 .....               | 16 |



# 1 简介

本文档介绍客户端在 AC 间漫游的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、802.1X 和 WLAN 特性。

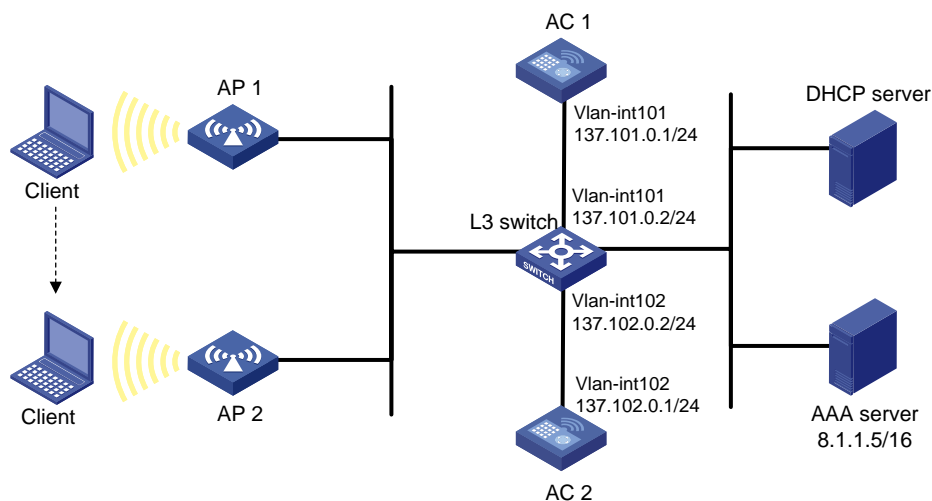
## 3 配置举例

### 3.1 组网需求

如图 1 所示, AP 1 和 AP 2 分别与 AC 1 和 AC 2 相连, DHCP 服务器为无线客户端和 AP 分配地址, 要求:

- 客户端需要通过 802.1X 认证才能上线。
- 配置无线客户端 AC 间漫游功能，实现无线客户端在 AP 1 和 AP 2 之间漫游时，所在 VLAN 不变，且无线客户端信息可以在 AC 1 和 AC 2 之间自动同步。
- 客户端在 AC 间漫游时不需要重新认证。
- 防止用户通过恶意假冒其它域账号从本端口接入网络。

图1 客户端在 AC 间漫游典型配置组网图



## 3.2 配置思路

- 由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。
- 为了防止用户通过恶意假冒其它域账号从本端口接入网络，配置端口的强制认证域。
- 由于无线客户端在跨 VLAN 漫游过程中需要通过 MAC VLAN 表项强制保持自身的 VLAN 不变，所以需要在 AC 上开启 MAC-VLAN 功能。
- 为了保证漫游成功，AC 1 和 AC 2 配置的 IACTP 隧道名称必须一致，且 AC 1 和 AC 2 配置的 IACTP 控制消息完整性认证模式和认证密码必须一致。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

#### (1) 配置 AC 1 的接口

# 创建 VLAN 101 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC1> system-view
[AC1] vlan 101
[AC1-vlan101] quit
[AC1] interface vlan-interface 101
[AC1-Vlan-interface101] ip address 137.101.0.1 24
[AC1-Vlan-interface101] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC1] vlan 200
[AC1-vlan200] quit
```

# VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC1] vlan 300
[AC1-vlan300] quit
```

# 配置默认路由。

```
[AC1] ip route-static 0.0.0.0 0 137.101.0.2
```

# 配置 AC 1 的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 101、VLAN 200 和 VLAN 300 通过。

```
[AC1] interface GigabitEthernet1/0/1
```

```
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 101 200 300
[AC1-GigabitEthernet1/0/1] quit
```

## (2) 配置 IACTP 隧道

# 创建 IACTP 隧道 office，并进入其视图。

```
[AC1] wlan mobility-group office
```

# 配置 IACTP 隧道的源 IP 地址。

```
[AC1-wlan-mg-office] source ip 137.101.0.1
```

# 配置 IACTP 隧道的成员 AC 2 的 IP 地址。

```
[AC1-wlan-mg-office] member ip 137.102.0.1
```

# 配置 IACTP 控制消息完整性认证模式为 md5，认证密码为 123456。

```
[AC1-wlan-mg-office] authentication-mode md5 simple 123456
```

# 开启 IACTP 隧道。

```
[AC1-wlan-mg-office] mobility-group enable
```

```
[AC1-wlan-mg-office] quit
```

## (3) 配置 802.1X 认证服务

# 使能端口安全。

```
[AC1] port-security enable
```

# 配置 802.1X 用户的认证方式为 EAP。

```
[AC1] dot1x authentication-method eap
```

## (4) 配置认证策略和认证域

# 创建 RADIUS 方案 office。

```
[AC1] radius scheme office
```

# 配置主认证 AAA 服务器的 IP 地址 8.1.1.5，主计费 AAA 服务器的 IP 地址 8.1.1.5。

```
[AC1-radius-office] primary authentication 8.1.1.5
```

```
[AC1-radius-office] primary accounting 8.1.1.5
```

# 配置 AC 1 与 AAA 认证服务器交互报文时的共享密钥为 123456789，与 AAA 计费服务器交互报文时的共享密钥为 123456789。

```
[AC1-radius-office] key authentication 123456789
```

```
[AC1-radius-office] key accounting 123456789
```

# 配置发送给 AAA 服务器的用户名不带 ISP 域名。

```
[AC1-radius-office] user-name-format without-domain
```

# 设置设备发送至 AAA 服务器的报文使用的源 IP 地址为 137.101.0.1

```
[AC1-radius-office] nas-ip 137.101.0.1
```

```
[AC1-radius-office] quit
```

# 添加认证域 office，并为该域指定对应的 RADIUS 认证方案为 office。

```
[AC1] domain office
```

```
[AC1-isp-office] authentication lan-access radius-scheme office
```

```
[AC1-isp-office] authorization lan-access radius-scheme none
```

```
[AC1-isp-office] accounting lan-access radius-scheme none
```

```
[AC1-isp-office] quit
```

## (5) 配置无线服务

# 创建 WLAN-ESS1 接口。

```
[AC1] interface wlan-ess 1
```

```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。
[AC1-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200, 禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC1-WLAN-ESS1] undo port hybrid vlan 1
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
# 配置 WLAN-ESS1 口开启 MAC-VLAN 功能。
[AC1-WLAN-ESS1] mac-vlan enable
# 配置 802.1X 用户的强制认证域为 office。
[AC1-WLAN-ESS1] dot1x mandatory-domain office
# 配置端口安全模式为 userlogin-secure-ext, 并使能端口 11key 类型的密钥协商功能。
[AC1-WLAN-ESS1] port-security port-mode userlogin-secure-ext
[AC1-WLAN-ESS1] port-security tx-key-type 11key
# 关闭 802.1X 多播触发功能和在线用户握手功能。
[AC1-WLAN-ESS1] undo dot1x multicast-trigger
[AC1-WLAN-ESS1] undo dot1x handshake
[AC1-WLAN-ESS1] quit
# 创建服务模板 1 (加密类型服务模板), 配置 SSID 为 service, 加密方式为 TKIP 和 AES-CCMP。
[AC1] wlan service-template 1 crypto
[AC1-wlan-st-1] ssid service
[AC1-wlan-st-1] bind wlan-ess 1
[AC1-wlan-st-1] authentication-method open-system
[AC1-wlan-st-1] cipher-suite tkip
[AC1-wlan-st-1] cipher-suite ccmp
# 设置在 AP 发送信标和探查响应帧时携带 RSN IE, 并使能服务模板。
[AC1-wlan-st-1] security-ie rsn
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit

```

#### (6) 配置射频接口并绑定服务模板

```

# 创建 AP 1 的模板, 名称为 officeap1, 型号名称选择 WA2620E-AGN, 并配置其序列号。
[AC1] wlan ap officeap1 model WA2620E-AGN
[AC1-wlan-ap-officeap1] serial-id 21023529G007C000020
# 设置 AP 1 的 radio 2 工作模式为 dot11gn, 将服务模板 1 绑定到该 radio 上, 设置绑定到射频接口的 VLAN 编号为 300, 并使能 radio。
[AC1-wlan-ap-officeap1] radio 2 type dot11gn
[AC1-wlan-ap-officeap1-radio-2] service-template 1 vlan-id 300
[AC1-wlan-ap-officeap1-radio-2] radio enable
[AC1-wlan-ap-officeap1-radio-2] quit
[AC1-wlan-ap-officeap1] quit

```

### 3.4.2 AC 2 的配置

#### (1) 配置 AC 2 的接口

```

# 创建 VLAN 102 及其对应的 VLAN 接口, 并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```

```

<AC2> system-view
[AC2] vlan 102
[AC2-vlan102] quit
[AC2] interface vlan-interface 102
[AC2-Vlan-interface102] ip address 137.102.0.1 24
[AC2-Vlan-interface102] quit
# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。
[AC2] vlan 200
[AC2-vlan200] quit
# 创建 VLAN 300 作为 Client 接入的业务 VLAN。
[AC2] vlan 300
[AC2-vlan300] quit
# 配置默认路由。
[AC2] ip route-static 0.0.0.0 0 137.102.0.2
# 配置 AC 2 的 GigabitEthernet1/0/1 接口的属性为 trunk, 允许 VLAN 102、VLAN 200 和 VLAN 300 通过。
[AC2] interface GigabitEthernet1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 102 200 300
[AC2-GigabitEthernet1/0/1] quit
(2) 配置 IACTP 隧道
# 创建 IACTP 隧道 office, 并进入其视图。
[AC2] wlan mobility-group office
# 配置 IACTP 隧道的源 IP 地址。
[AC2-wlan-mg-office] source ip 137.102.0.1
# 配置 IACTP 隧道的成员 AC 1 的 IP 地址。
[AC2-wlan-mg-office] member ip 137.101.0.1
# 配置 IACTP 控制消息完整性认证模式为 md5, 认证密码为 123456。
[AC2-wlan-mg-office] authentication-mode md5 simple 123456
# 开启 IACTP 隧道。
[AC2-wlan-mg-office] mobility-group enable
[AC2-wlan-mg-office] quit
(3) 配置 802.1X 认证服务
# 使能端口安全。
[AC2] port-security enable
# 配置 802.1X 用户的认证方式为 EAP。
[AC2] dot1x authentication-method eap
(4) 配置认证策略和认证域
# 创建 RADIUS 方案 office。
[AC2] radius scheme office
# 配置主认证 AAA 服务器的 IP 地址 8.1.1.5, 主计费 AAA 服务器的 IP 地址 8.1.1.5。
[AC2-radius-office] primary authentication 8.1.1.5
[AC2-radius-office] primary accounting 8.1.1.5

```

# 配置 AC 与 AAA 认证服务器交互报文时的共享密钥为 123456789，与 AAA 计费服务器交互报文时的共享密钥为 123456789。

```
[AC2-radius-office] key authentication 123456789
```

```
[AC2-radius-office] key accounting 123456789
```

# 配置 AC 发送给 AAA 服务器的用户名不带 ISP 域名。

```
[AC2-radius-office] user-name-format without-domain
```

# 设置设备发送至 AAA 服务器的报文使用的源 IP 地址为 137.102.0.1。

```
[AC2-radius-office] nas-ip 137.102.0.1
```

```
[AC2-radius-office] quit
```

# 添加认证域 office，并为该域指定对应的 RADIUS 认证方案为 office。

```
[AC2] domain office
```

```
[AC2-isp-office] authentication lan-access radius-scheme office
```

```
[AC2-isp-office] authorization lan-access radius-scheme none
```

```
[AC2-isp-office] accounting lan-access radius-scheme none
```

```
[AC2-isp-office] quit
```

## (5) 配置无线服务

# 创建 WLAN-ESS1 接口。

```
[AC2] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC2-WLAN-ESS1] port link-type hybrid
```

# 配置当前 hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC2-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
```

# 配置 WLAN-ESS1 口开启 MAC-VLAN 功能。

```
[AC2-WLAN-ESS1] mac-vlan enable
```

# 在接口 WLAN-ESS1 上配置 802.1X 用户的强制认证域 office。

```
[AC2-WLAN-ESS1] dot1x mandatory-domain office
```

# 配置端口安全模式为 userlogin-secure-ext，并使能端口 11key 类型的密钥协商功能。

```
[AC2-WLAN-ESS1] port-security port-mode userlogin-secure-ext
```

```
[AC2-WLAN-ESS1] port-security tx-key-type 11key
```

# 关闭 802.1X 多播触发功能和在线用户握手功能。

```
[AC2-WLAN-ESS1] undo dot1x multicast-trigger
```

```
[AC2-WLAN-ESS1] undo dot1x handshake
```

```
[AC2-WLAN-ESS1] quit
```

# 创建服务模板 1（加密类型服务模板），配置 SSID 为 service，加密方式为 TKIP 和 AES-CCMP。

```
[AC2] wlan service-template 1 crypto
```

```
[AC2-wlan-st-1] ssid service
```

```
[AC2-wlan-st-1] bind wlan-ess 1
```

```
[AC2-wlan-st-1] authentication-method open-system
```

```
[AC2-wlan-st-1] cipher-suite tkip
```

```
[AC2-wlan-st-1] cipher-suite ccmp
```

# 设置在 AP 发送信标和探查响应帧时携带 RSN IE，并使能服务模板。

```
[AC2-wlan-st-1] security-ie rsn
```

```
[AC2-wlan-st-1] service-template enable
```

```
[AC2-wlan-st-1] quit
```

#### (6) 配置射频接口并绑定服务模板

# 创建 AP 2 的模板，名称为 officeap2，型号名称选择 WA2620E-AGN，并配置其序列号。

```
[AC2] wlan ap officeap2 model WA2620E-AGN
```

```
[AC2-wlan-ap-officeap2] serial-id 21023529G007C000021
```

# 进入射频 2 视图，将服务模板 1 绑定到该 radio 上，设置绑定到射频接口的 VLAN 编号为 300，并使能 radio。

```
[AC2-wlan-ap-officeap2] radio 2
```

```
[AC2-wlan-ap-officeap2-radio-2] service-template 1 vlan-id 300
```

```
[AC2-wlan-ap-officeap2-radio-2] radio enable
```

```
[AC2-wlan-ap-officeap2-radio-2] quit
```

```
[AC2-wlan-ap-officeap2] quit
```

### 3.4.3 L3 switch 的配置

# 创建 VLAN 101、VLAN 102、和 VLAN 300，其中 VLAN 101 和 VLAN 102 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 101
```

```
[Switch-vlan101] quit
```

```
[Switch] vlan 102
```

```
[Switch-vlan102] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 1 相连的 GigabitEthernet1/0/1 接口的属性为 trunk，当前 trunk 口的 PVID 为 101，允许 VLAN 101、300 通过。

```
[Switch] interface GigabitEthernet1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 101 300
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 101
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AC 2 相连的 GigabitEthernet1/0/2 接口的属性为 trunk，当前 trunk 口的 PVID 为 102，允许 VLAN 102、300 通过。

```
[Switch] interface GigabitEthernet1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 102 300
```

```
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 102
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/3 接口属性为 access，并允许 VLAN 101 通过。

```
[Switch] interface GigabitEthernet1/0/3
```

```
[Switch-GigabitEthernet1/0/3] port link-type access
```

```
[Switch-GigabitEthernet1/0/3] port access vlan 101
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/3] poe enable
```

```
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/4 接口属性为 access，并允许 VLAN 102 通过。

```
[Switch] interface GigabitEthernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 102
# 使能 PoE 功能。
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
# 配置 VLAN 101 接口的 IP 地址为 137.101.0.2/24，VLAN 102 接口的 IP 地址为 137.102.0.2/24。
[Switch] interface vlan-interface 101
[Switch-Vlan-interface101] ip address 137.101.0.2 255.255.255.0
[Switch-Vlan-interface101] quit
[Switch] interface vlan-interface 102
[Switch-Vlan-interface102] ip address 137.102.0.2 255.255.255.0
[Switch-Vlan-interface102] quit
```

### 3.4.4 AAA server 的配置



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)），说明 AAA server 的基本配置。

# 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置认证、计费共享密钥为 123456789，其它保持缺省配置；
- 选择或手工增加接入设备，添加 IP 地址为 137.101.0.1 和 137.102.0.1 的接入设备。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

接入配置

|        |              |          |         |
|--------|--------------|----------|---------|
| 认证端口 * | 1812         | 计费端口 *   | 1813    |
| 组网方式   | 不启用混合组网      | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 接入设备分组   | 无       |
| 共享密钥 * | *****        | 确认共享密钥 * | *****   |
| 业务分组   | 未分组          |          |         |

设备列表

| 选择 | 手工增加 | 全部清除 | 设备名称 | 设备IP地址      | 设备型号 | 备注 | 删除 |
|----|------|------|------|-------------|------|----|----|
|    |      |      |      | 137.102.0.1 |      |    | 删除 |
|    |      |      |      | 137.101.0.1 |      |    | 删除 |

共有2条记录。

确定 取消

# 增加接入策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击<增加>按钮，进入增加接入策略页面。

- 设置接入策略名为 office；



- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证。

图3 增加接入策略页面

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 \* office

业务分组 \* 未分组

描述

授权信息

接入时段 无 分配IP地址 \* 否

下行速率(Kbps)

上行速率(Kbps)

优先级

证书认证 ☐ 不启用 ☒ EAP证书认证 ☐ WAP证书认证

认证证书类型 EAP-PEAP认证

认证证书子类型 MS-CHAPV2认证

下发VLAN

☐ 下发User Profile

☐ 下发ACL

下发用户组

认证绑定信息

☐ 绑定接入设备IP ☐ 绑定接入设备端口 ☐ 绑定VLAN ☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址 ☐ 绑定用户MAC地址 ☐ 绑定IMSI号码 ☐ 绑定计算机名称

☐ 计算机绑定域 ☐ 用户必须登录到域 ☐ 绑定无线SSID ☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制 ☐ 启用终端硬盘序列号控制 ☐ 启用无线SSID控制

# 增加接入服务。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 设置服务名为 office；
- 选择缺省接入策略为 office，其他保持缺省配置。

图4 增加接入服务页面

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 \* office

业务分组 \* 未分组

缺省安全策略 \* 不使用

缺省私有属性下发策略 \* 不使用

缺省BYOD页面 \* PC-缺省页面 (PC)

服务描述

☒ 可申请 ☐ Portal无感知认证

服务后缀

缺省接入策略 \* office

缺省内网外联配置 \* 不使用

接入场景列表

增加

| 名称          | 接入策略 | 安全策略 | 私有属性下发策略 | 内网外联配置 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|------|----------|--------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |      |          |        |        |     |    |    |

确定 取消

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 单击<增加用户>添加用户 office，证件号码 123456；
- 添加帐号名为 office，密码为 123456；
- 选中刚才配置的服务 office。

图5 增加接入用户

用户姓名 \*

office

选择

增加用户

帐号名 \*

office

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                        | 服务后缀 | 缺省安全策略  | 状态  | 分配IP地址 |
|--------------------------------------------|------|---------|-----|--------|
| <input type="checkbox"/> 802.1x            |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> 802-eap           |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> k4166             |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> lw_802.1x         |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> mpc_ead           |      | mpc_ead | 可申请 |        |
| <input type="checkbox"/> mpc_peap          |      | 不使用     | 可申请 |        |
| <input checked="" type="checkbox"/> office |      | 不使用     | 可申请 |        |

3.5 验证配置

# 客户端首先从 AC 1 下连接的 officeap1 的 VLAN 300 上线。通过 **display wlan client verbose** 命令可以看到客户端的详细信息。

```
[AC1] display wlan client verbose
Total Number of Clients          : 1
Client Information
-----
MAC Address                      : 0015-00ef-ac23
User Name                       : office
IP Address                      : 0.0.0.0
AID                             : 1
AP Name                         : officeap1
Radio Id                       : 2
Antenna Id                     : 0
Service Template Number        : 1
SSID                           : service
BSSID                          : c8cb-b8f1-f6d0
Port                            : WLAN-DBSS1:1
VLAN                            : 300
State                           : Running
Power Save Mode                 : Active
Wireless Mode                   : 11g
QoS Mode                       : WMM
Listen Interval (Beacon Interval) : 10
RSSI                            : 42
Rx/Tx Rate                     : 48/36
Client Type                     : WPA2(RSN)
Authentication Method           : Open System
```

```

Authentication Mode          : Central
AKM Method                   : Dot1X
4-Way Handshake State       : PTKINITDONE
Group Key State              : IDLE
Encryption Cipher            : AES-CCMP
Roam Status                  : Normal
Roam Count                   : 0
Up Time (hh:mm:ss)          : 00:00:51

```

# 通过 **display wlan mobility-group** 命令可以查看 IACTP 隧道信息。

```
[AC1] display wlan mobility-group
```

#### Mobility Group Information

```

Group Name       : office
Source IP Address : 137.101.0.1
Authentication Method : MD5

```

#### Member Information

| IP-address  | State | Interface    |
|-------------|-------|--------------|
| 137.102.0.1 | Run   | WLAN-Tunnel2 |

```
[AC2] display wlan mobility-group
```

#### Mobility Group Information

```

Group Name       : office
Source IP Address : 137.102.0.1
Authentication Method : MD5

```

#### Member Information

| IP-address  | State | Interface    |
|-------------|-------|--------------|
| 137.101.0.1 | Run   | WLAN-Tunnel2 |

# 当客户端从 AC 1 下连接的 AP 1 漫游至 AC 2 下连接的 AP 2 上时，客户端信息同步到 AC 2，客户端不需要重新进行认证，客户端初始 VLAN 300 也被同步过来。通过 **display wlan client verbose** 命令在 AC 2 上显示客户端进行 AC 间漫游，信息如下：

```
[AC2] display wlan client verbose
```

```
Total Number of Clients      : 1
```

#### Client Information

```

MAC Address       : 0015-00ef-ac23
User Name         : office
IP Address        : 0.0.0.0
AID               : 2
AP Name           : officeap2

```

```

Radio Id                : 2
Antenna Id              : 0
Service Template Number : 1
SSID                    : service
BSSID                   : 0023-8930-9010
Port                    : WLAN-DBSS1:1
VLAN                    : 300
State                   : Running
Power Save Mode         : Active
Wireless Mode           : 11g
QoS Mode                : WMM
Listen Interval (Beacon Interval) : 10
RSSI                    : 42
Rx/Tx Rate              : 48/36
Client Type             : WPA2(RSN)
Authentication Method    : Open System
Authentication Mode      : Central
AKM Method              : Dot1X
4-Way Handshake State   : PTKINITDONE
Group Key State          : IDLE
Encryption Cipher        : AES-CCMP
Roam Status              : Inter-AC roam association
Roam Count               : 1
Up Time (hh:mm:ss)      : 00:17:51

```

-----

**# AC 1 上查询客户端漫游追踪信息，显示 Client 当前已经漫游至 AC 2:**

```
[AC1] display wlan client roam-track mac-address 0015-00ef-ac23
```

```

-----
BSSID           Online-time(d:h:m:s) AC-IP-address
-----
0023-8930-9010  0000:00:21:19          137.102.0.1
c8cb-b8f1-f6d0  0000:00:19:14          137.101.0.1 (HOME AC)

```

## 3.6 配置文件

- AC 1:
 

```

#
port-security enable
#
dot1x authentication-method eap
#
vlan 101
#
vlan 200
#
vlan 300
#
radius scheme office

```

```

primary authentication 8.1.1.5
primary accounting 8.1.1.5
key authentication cipher $c$3$SjWMEAJbTjqCC9+XhRLYhNZOSJ6bBN/7K3HBEA==
key accounting cipher $c$3$Oj5WtaBGNaZb9s+R0Y/z0yKMG4fZcS0LuOUeOw==
user-name-format without-domain
nas-ip 137.101.0.1
#
domain office
authentication lan-access radius-scheme office
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 1
cipher-suite tkip
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 101 200 300
#
interface Vlan-interface101
ip address 137.101.0.1 255.255.255.0
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
port-security port-mode userlogin-secure-ext
port-security tx-key-type 11key
undo dot1x handshake
dot1x mandatory-domain office
undo dot1x multicast-trigger
#
wlan ap officeap1 model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1 vlan-id 300
radio enable
#

```

```

wlan mobility-group office
  member ip 137.102.0.1
  source ip 137.101.0.1
  authentication-mode MD5 cipher $c$3$0ltSGsSqV3ls4QJM7n6PXHtOFKFDSc3d9Q==
  mobility-group enable
#
ip route-static 0.0.0.0 0.0.0.0 137.101.0.2
#
•   AC 2:
#
  port-security enable
#
  dot1x authentication-method eap
#
vlan 102
#
vlan 200
#
vlan 300
#
radius scheme office
  primary authentication 8.1.1.5
  primary accounting 8.1.1.5
  key authentication cipher $c$3$SjWMEAjbtjqCC9+XHRLYhNZOSJ6bBN/7K3HBEA==
  key accounting cipher $c$3$Oj5WtaBGNaZb9s+R0Y/z0yKMG4fZcS0LuOUeOw==
  user-name-format without-domain
  nas-ip 137.102.0.1
#
domain office
  authentication lan-access radius-scheme office
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#
wlan service-template 1 crypto
  ssid service
  bind WLAN-ESS 1
  cipher-suite tkip
  cipher-suite ccmp
  security-ie rsn
  service-template enable
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 102 200 300
#
interface Vlan-interface102

```

```

ip address 137.102.0.1 255.255.255.0
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
port-security port-mode userlogin-secure-ext
port-security tx-key-type 11key
undo dot1x handshake
dot1x mandatory-domain office
undo dot1x multicast-trigger
#
wlan ap officeap2 model WA2620E-AGN id 1
serial-id 21023529G007C000021
radio 1
radio 2
service-template 1 vlan-id 300
radio enable
#
wlan mobility-group office
member ip 137.101.0.1
source ip 137.102.0.1
authentication-mode MD5 cipher $c$3$0ltSGsSqV3ls4QJM7n6PXHtOFKFDS3d9Q==
mobility-group enable
#
ip route-static 0.0.0.0 0.0.0.0 137.102.0.2
#

```

- **Switch:**

```

#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
ip address 137.101.0.2 255.255.255.0
#
interface Vlan-interface102
ip address 137.102.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 101 300
port trunk pvid vlan 101
#
interface GigabitEthernet1/0/2

```

```
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 102 300
port trunk pvid vlan 102
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 101
poe enable
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 102
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。



# IPv6 客户端在 AC 间漫游典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                               |    |
|-------------------------------|----|
| 1 简介.....                     | 1  |
| 2 配置前提 .....                  | 1  |
| 3 配置举例 .....                  | 1  |
| 3.1 组网需求 .....                | 1  |
| 3.2 配置思路 .....                | 2  |
| 3.3 配置注意事项.....               | 2  |
| 3.4 配置步骤 .....                | 3  |
| 3.4.1 AC 1 的配置 .....          | 3  |
| 3.4.2 AC 2 的配置 .....          | 5  |
| 3.4.3 L3 switch 的配置 .....     | 7  |
| 3.4.4 DHCPv6 server 的配置 ..... | 9  |
| 3.4.5 AAA server 的配置 .....    | 10 |
| 3.5 验证配置 .....                | 12 |
| 3.6 配置文件 .....                | 15 |
| 4 相关资料 .....                  | 19 |

# 1 简介

本文档介绍客户端在 AC 间漫游的 IPv6 典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V5 软件版本的无线控制器和接入点产品，不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 DHCPv6、AAA、802.1X 和 WLAN 特性。

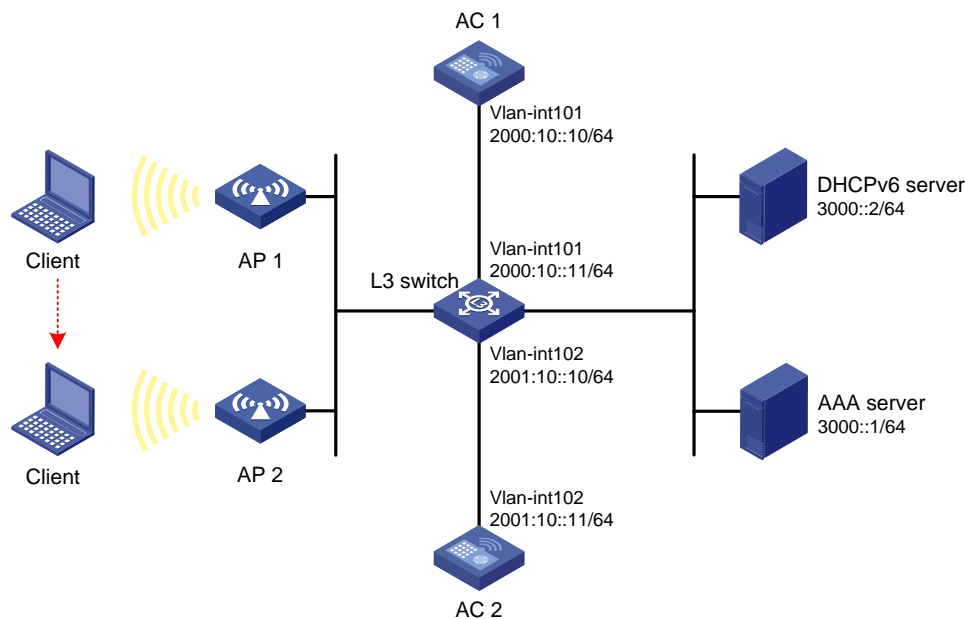
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示, AP 1 和 AP 2 分别与 AC 1 和 AC 2 相连, DHCPv6 服务器为无线客户端和 AP 分配 IPv6 地址, 要求:

- 客户端需要通过 802.1X 认证才能上线。
- 配置无线客户端 AC 间漫游功能, 实现无线客户端在 AP 1 和 AP 2 之间漫游时, 所在 VLAN 不变, 且无线客户端信息可以在 AC 1 和 AC 2 之间自动同步。
- 客户端在 AC 间漫游时不需要重新认证。
- 防止用户通过恶意假冒其它域账号从本端口接入网络。

图1 客户端在 AC 间漫游 IPv6 典型配置组网图



## 3.2 配置思路

- 由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。
- 为了防止用户通过恶意假冒其它域账号从本端口接入网络，配置端口的强制认证域。
- 由于无线客户端在跨 VLAN 漫游过程中需要通过 MAC VLAN 表项强制保持自身的 VLAN 不变，所以需要在 AC 上开启 MAC-VLAN 功能。
- 为了保证漫游成功，AC 1 和 AC 2 配置的 IACTP 隧道名称必须一致，且 AC 1 和 AC 2 配置的 IACTP 控制消息完整性认证模式和认证密码必须一致。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

#### (1) 配置 AC 1 的接口

# 创建 VLAN 101 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。AC 将使用该接口的 IPv6 地址与 AP 建立 LWAPP 隧道。

```
<AC1> system-view
[AC1] vlan 101
[AC1-vlan101] quit
[AC1] interface vlan-interface 101
[AC1-Vlan-interface101] ipv6 address 2000:10::10/64
[AC1-Vlan-interface101] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC1] vlan 200
[AC1-vlan200] quit
```

# VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC1] vlan 300
[AC1-vlan300] quit
```

# 配置默认路由。

```
[AC1] ipv6 route-static 0::0 64 2000:10::11
```

# 配置 AC 1 的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 101、VLAN 200 和 VLAN 300 通过。

```
[AC1] interface GigabitEthernet1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 101 200 300
[AC1-GigabitEthernet1/0/1] quit
```

#### (2) 配置 IACTP 隧道

# 创建 IACTP 隧道 office，并进入其视图。

```
[AC1] wlan mobility-group office
```

# 配置 IACTP 隧道类型为 IPv6。

```
[AC1-wlan-mg-office] mobility-tunnel iactp6
```

# 配置 IACTP 隧道的源 IPv6 地址。

```
[AC1-wlan-mg-office] source ipv6 2000:10::10
```

# 配置 IACTP 隧道的成员 AC 2 的 IPv6 地址。

```
[AC1-wlan-mg-office] member ipv6 2001:10::11
```

# 配置 IACTP 控制消息完整性认证模式为 md5，认证密码为 123456。

```
[AC1-wlan-mg-office] authentication-mode md5 simple 123456
```

# 开启 IACTP 隧道。

```
[AC1-wlan-mg-office] mobility-group enable
[AC1-wlan-mg-office] quit
```

#### (3) 配置 802.1X 认证服务

# 使能端口安全。

```
[AC1] port-security enable
```

# 配置 802.1X 用户的认证方式为 EAP。

```
[AC1] dot1x authentication-method eap
```

#### (4) 配置认证策略和认证域

# 创建 RADIUS 方案 office。

```
[AC1] radius scheme office
```

# 配置主认证 AAA 服务器的 IPv6 地址 3000::1，主计费 AAA 服务器的 IPv6 地址 3000::1。

```
[AC1-radius-office] primary authentication ipv6 3000::1
```

```
[AC1-radius-office] primary accounting ipv6 3000::1
```

# 配置 AC 1 与 AAA 认证服务器交互报文时的共享密钥为 123456789，与 AAA 计费服务器交互报文时的共享密钥为 123456789。

```
[AC1-radius-office] key authentication 123456789
```

```
[AC1-radius-office] key accounting 123456789
```

# 配置发送给 AAA 服务器的用户名不带 ISP 域名。

```
[AC1-radius-office] user-name-format without-domain
```

# 设置设备发送至 AAA 服务器的报文使用的源 IPv6 地址为 2000:10::10

```
[AC1-radius-office] nas-ip ipv6 2000:10::10
```

```
[AC1-radius-office] quit
```

# 添加认证域 office，并为该域指定对应的 RADIUS 认证方案为 office。

```
[AC1] domain office
```

```
[AC1-isp-office] authentication lan-access radius-scheme office
```

```
[AC1-isp-office] authorization lan-access radius-scheme none
```

```
[AC1-isp-office] accounting lan-access radius-scheme none
```

```
[AC1-isp-office] quit
```

#### (5) 配置无线服务

# 创建 WLAN-ESS1 接口。

```
[AC1] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC1-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC1-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
```

# 配置 WLAN-ESS1 口开启 MAC-VLAN 功能。

```
[AC1-WLAN-ESS1] mac-vlan enable
```

# 配置 802.1X 用户的强制认证域为 office。

```
[AC1-WLAN-ESS1] dot1x mandatory-domain office
```

# 配置端口安全模式为 userlogin-secure-ext，并使能端口 11key 类型的密钥协商功能。

```
[AC1-WLAN-ESS1] port-security port-mode userlogin-secure-ext
```

```
[AC1-WLAN-ESS1] port-security tx-key-type 11key
```

# 关闭 802.1X 多播触发功能和在线用户握手功能。

```
[AC1-WLAN-ESS1] undo dot1x multicast-trigger
```

```
[AC1-WLAN-ESS1] undo dot1x handshake
```

```
[AC1-WLAN-ESS1] quit
```

# 创建服务模板 1（加密类型服务模板），配置 SSID 为 service，加密方式为 TKIP 和 AES-CCMP。

```
[AC1] wlan service-template 1 crypto
[AC1-wlan-st-1] ssid service
[AC1-wlan-st-1] bind wlan-ess 1
[AC1-wlan-st-1] authentication-method open-system
[AC1-wlan-st-1] cipher-suite tkip
[AC1-wlan-st-1] cipher-suite ccmp
# 设置在 AP 发送信标和探查响应帧时携带 RSN IE 和 WPA IE，并使能服务模板。
[AC1-wlan-st-1] security-ie rsn
[AC1-wlan-st-1] security-ie wpa
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
```

#### (6) 配置射频接口并绑定服务模板

# 创建 AP 1 的模板，名称为 officeap1，型号名称选择 WA2620E-AGN，并配置其序列号。

```
[AC1] wlan ap officeap1 model WA2620E-AGN
[AC1-wlan-ap-officeap1] serial-id 21023529G007C000020
```

# 设置 AP 1 的 radio 2 工作模式为 dot11gn，将服务模板 1 绑定到该 radio 上，设置绑定到射频接口的 VLAN 编号为 300，并使能 radio。

```
[AC1-wlan-ap-officeap1] radio 2 type dot11gn
[AC1-wlan-ap-officeap1-radio-2] service-template 1 vlan-id 300
[AC1-wlan-ap-officeap1-radio-2] radio enable
[AC1-wlan-ap-officeap1-radio-2] quit
[AC1-wlan-ap-officeap1] quit
```

### 3.4.2 AC 2 的配置

#### (1) 配置 AC 2 的接口

# 创建 VLAN 102 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。AC 将使用该接口的 IPv6 地址与 AP 建立 LWAPP 隧道。

```
<AC2> system-view
[AC2] vlan 102
[AC2-vlan102] quit
[AC2] interface vlan-interface 102
[AC2-Vlan-interface102] ipv6 address 2001:10::11/64
[AC2-Vlan-interface102] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC2] vlan 200
[AC2-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC2] vlan 300
[AC2-vlan300] quit
```

# 配置默认路由。

```
[AC2] ipv6 route-static 0::0 64 2001:10::10
```

# 配置 AC 2 的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 102、VLAN 200 和 VLAN 300 通过。

```
[AC2] interface GigabitEthernet1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 102 200 300
[AC2-GigabitEthernet1/0/1] quit
```

## (2) 配置 IACTP 隧道

# 创建 IACTP 隧道 office，并进入其视图。

```
[AC2] wlan mobility-group office
```

# 配置 IACTP 隧道类型为 IPv6。

```
[AC2-wlan-mg-office] mobility-tunnel iactp6
```

# 配置 IACTP 隧道的源 IPv6 地址。

```
[AC2-wlan-mg-office] source ipv6 2001:10::11
```

# 配置 IACTP 隧道的成员 AC 1 的 IPv6 地址。

```
[AC2-wlan-mg-office] member ipv6 2000:10::10
```

# 配置 IACTP 控制消息完整性认证模式为 md5，认证密码为 123456。

```
[AC2-wlan-mg-office] authentication-mode md5 simple 123456
```

# 开启 IACTP 隧道。

```
[AC2-wlan-mg-office] mobility-group enable
```

```
[AC2-wlan-mg-office] quit
```

## (3) 配置 802.1X 认证服务

# 使能端口安全。

```
[AC2] port-security enable
```

# 配置 802.1X 用户的认证方式为 EAP。

```
[AC2] dot1x authentication-method eap
```

## (4) 配置认证策略和认证域

# 创建 RADIUS 方案 office。

```
[AC2] radius scheme office
```

# 配置主认证 AAA 服务器的 IPv6 地址 3000::1，主计费 AAA 服务器的 IPv6 地址 3000::1。

```
[AC2-radius-office] primary authentication ipv6 3000::1
```

```
[AC2-radius-office] primary accounting ipv6 3000::1
```

# 配置 AC 与 AAA 认证服务器交互报文时的共享密钥为 123456789，与 AAA 计费服务器交互报文时的共享密钥为 123456789。

```
[AC2-radius-office] key authentication 123456789
```

```
[AC2-radius-office] key accounting 123456789
```

# 配置 AC 发送给 AAA 服务器的用户名不带 ISP 域名。

```
[AC2-radius-office] user-name-format without-domain
```

# 设置设备发送至 AAA 服务器的报文使用的源 IPv6 地址为 2001:10::11。

```
[AC2-radius-office] nas-ip ipv6 2001:10::11
```

```
[AC2-radius-office] quit
```

# 添加认证域 office，并为该域指定对应的 RADIUS 认证方案为 office。

```
[AC2] domain office
```

```
[AC2-isp-office] authentication lan-access radius-scheme office
```

```
[AC2-isp-office] authorization lan-access radius-scheme none
```

```
[AC2-isp-office] accounting lan-access radius-scheme none
```

```
[AC2-isp-office] quit
```

## (5) 配置无线服务

# 创建 WLAN-ESS1 接口。



```

[AC2] interface wlan-ess 1
# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。
[AC2-WLAN-ESS1] port link-type hybrid
# 配置当前 hybrid 端口的 PVID 为 VLAN 200, 禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC2-WLAN-ESS1] undo port hybrid vlan 1
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
# 配置 WLAN-ESS1 口开启 MAC-VLAN 功能。
[AC2-WLAN-ESS1] mac-vlan enable
# 在接口 WLAN-ESS1 上配置 802.1X 用户的强制认证域 office。
[AC2-WLAN-ESS1] dot1x mandatory-domain office
# 配置端口安全模式为 userlogin-secure-ext, 并使能端口 11key 类型的密钥协商功能。
[AC2-WLAN-ESS1] port-security port-mode userlogin-secure-ext
[AC2-WLAN-ESS1] port-security tx-key-type 11key
# 关闭 802.1X 多播触发功能和在线用户握手功能。
[AC2-WLAN-ESS1] undo dot1x multicast-trigger
[AC2-WLAN-ESS1] undo dot1x handshake
[AC2-WLAN-ESS1] quit
# 创建服务模板 1 (加密类型服务模板), 配置 SSID 为 service, 加密方式为 TKIP 和 AES-CCMP。
[AC2] wlan service-template 1 crypto
[AC2-wlan-st-1] ssid service
[AC2-wlan-st-1] bind wlan-ess 1
[AC2-wlan-st-1] authentication-method open-system
[AC2-wlan-st-1] cipher-suite tkip
[AC2-wlan-st-1] cipher-suite ccmp
# 设置在 AP 发送信标和探查响应帧时携带 RSN IE 和 WPA IE, 并使能服务模板。
[AC2-wlan-st-1] security-ie rsn
[AC2-wlan-st-1] security-ie wpa
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
(6) 配置射频接口并绑定服务模板
# 创建 AP 2 的模板, 名称为 officeap2, 型号名称选择 WA2620E-AGN, 并配置其序列号。
[AC2] wlan ap officeap2 model WA2620E-AGN
[AC2-wlan-ap-officeap2] serial-id 21023529G007C000021
# 进入射频 2 视图, 将服务模板 1 绑定到该 radio 上, 设置绑定到射频接口的 VLAN 编号为 300, 并使能 radio。
[AC2-wlan-ap-officeap2] radio 2
[AC2-wlan-ap-officeap2-radio-2] service-template 1 vlan-id 300
[AC2-wlan-ap-officeap2-radio-2] radio enable
[AC2-wlan-ap-officeap2-radio-2] quit
[AC2-wlan-ap-officeap2] quit

```

### 3.4.3 L3 switch 的配置

# 创建 VLAN 101、VLAN 102、和 VLAN 300, 其中 VLAN 101 和 VLAN 102 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线用户接入的 VLAN。

```

<Switch> system-view
[Switch] vlan 101
[Switch-vlan101] quit
[Switch] vlan 102
[Switch-vlan102] quit
[Switch] vlan 300
[Switch-vlan300] quit

```

**# 配置 Switch 与 AC 1 相连的 GigabitEthernet1/0/1 接口的属性为 trunk，当前 trunk 口的 PVID 为 101，允许 VLAN 101、300 通过。**

```

[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 101 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 101
[Switch-GigabitEthernet1/0/1] quit

```

**# 配置 Switch 与 AC 2 相连的 GigabitEthernet1/0/2 接口的属性为 trunk，当前 trunk 口的 PVID 为 102，允许 VLAN 102、300 通过。**

```

[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 102 300
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 102
[Switch-GigabitEthernet1/0/2] quit

```

**# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/3 接口属性为 access，并允许 VLAN 101 通过。**

```

[Switch] interface GigabitEthernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 101

```

**# 使能 PoE 功能。**

```

[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit

```

**# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/4 接口属性为 access，并允许 VLAN 102 通过。**

```

[Switch] interface GigabitEthernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 102

```

**# 使能 PoE 功能。**

```

[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit

```

**# 配置 VLAN 101 接口的 IPv6 地址为 2000:10::11/64，VLAN 102 接口的 IPv6 地址为 2001:10::10/64。**

```

[Switch] interface vlan-interface 101
[Switch-Vlan-interface101] ipv6 address 2000:10::11/64
[Switch-Vlan-interface101] quit
[Switch] interface vlan-interface 102
[Switch-Vlan-interface102] ipv6 address 2001:10::10/64
[Switch-Vlan-interface102] quit

```

**# 配置 Switch 与 DHCPv6 server 相连的 GigabitEthernet1/0/5 接口的 IPv6 地址为 3000::3/64。**

```

[Switch] interface gigabitethernet 1/0/5
[Switch-GigabitEthernet1/0/5] ipv6 address 3000::3/64
[Switch-GigabitEthernet1/0/5] quit

```

### 3.4.4 DHCPv6 server 的配置

#### (1) 配置 DHCPv6 server 的接口

# 配置 DHCPv6 server 与 Swtich 相连的 GigabitEthernet1/0/1 接口的 IPv6 地址为 3000::2/64。

```
<DHCPv6 server> system-view
[DHCPv6 server] interface gigabitethernet 1/0/1
[DHCPv6 server-GigabitEthernet1/0/1] ipv6 address 3000::2/64
[DHCPv6 server-GigabitEthernet1/0/1] quit
```

# 创建 VLAN 101 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。

```
[DHCPv6 server] vlan 101
[DHCPv6 server-vlan101] quit
[DHCPv6 server] interface vlan-interface 101
[DHCPv6 server-Vlan-interface101] ipv6 address 2000:10::1/64
```

# 配置 VLAN 接口 101 工作在 DHCPv6 服务器模式，并引用地址池 101，配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```
[DHCPv6 server-Vlan-interface101] ipv6 dhcp server apply pool 101
[DHCPv6 server-Vlan-interface101] ipv6 nd autoconfig managed-address-flag
[DHCPv6 server-Vlan-interface101] ipv6 nd autoconfig other-flag
[DHCPv6 server-Vlan-interface101] quit
```

# 创建 VLAN 102 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。

```
[DHCPv6 server] vlan 102
[DHCPv6 server-vlan102] quit
[DHCPv6 server] interface vlan-interface 102
[DHCPv6 server-Vlan-interface102] ipv6 address 2001:10::1/64
```

# 配置 VLAN 接口 102 工作在 DHCPv6 服务器模式，并引用地址池 102，配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```
[DHCPv6 server-Vlan-interface102] ipv6 dhcp server apply pool 102
[DHCPv6 server-Vlan-interface102] ipv6 nd autoconfig managed-address-flag
[DHCPv6 server-Vlan-interface102] ipv6 nd autoconfig other-flag
[DHCPv6 server-Vlan-interface102] quit
```

# 创建 VLAN 300 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。

```
[DHCPv6 server] vlan 300
[DHCPv6 server-vlan300] quit
[DHCPv6 server] interface vlan-interface 300
[DHCPv6 server-Vlan-interface300] ipv6 address 2002:10::1/64
```

# 配置 VLAN 接口 300 工作在 DHCPv6 服务器模式，并引用地址池 300，配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```
[DHCPv6 server-Vlan-interface300] ipv6 dhcp server apply pool 300
[DHCPv6 server-Vlan-interface300] ipv6 nd autoconfig managed-address-flag
[DHCPv6 server-Vlan-interface300] ipv6 nd autoconfig other-flag
[DHCPv6 server-Vlan-interface300] quit
```

# 配置默认路由。

```
[DHCPv6 server] ipv6 route-static 0::0 64 3000::2
```

## (2) 配置 DHCPv6 服务

# 开启 IPv6 报文转发和 DHCPv6 服务器功能。

```
[DHCPv6 server] ipv6
```

```
[DHCPv6 server] ipv6 dhcp server enable
```

# 配置 DHCPv6 地址池 VLAN 101 为 AP 1 动态分配的网段为 2000:10::0/64, 网关地址为 2000:10::1。

```
[DHCPv6 server] ipv6 dhcp pool vlan 101
```

```
[DHCPv6 server-dhcp6-pool-vlan101] network 2000:10::0 64
```

```
[DHCPv6 server-dhcp6-pool-vlan101] gateway-list 2000:10::1
```

```
[DHCPv6 server-dhcp6-pool-vlan101] quit
```

# 配置 DHCPv6 地址池 VLAN 102 为 AP 2 动态分配的网段为 2001:10::0/64, 网关地址为 2001:10::1。

```
[DHCPv6 server] ipv6 dhcp pool vlan 102
```

```
[DHCPv6 server-dhcp6-pool-vlan102] network 2001:10::0 64
```

```
[DHCPv6 server-dhcp6-pool-vlan102] gateway-list 2001:10::1
```

```
[DHCPv6 server-dhcp6-pool-vlan102] quit
```

# 配置 DHCPv6 地址池 VLAN 300 为 Client 动态分配的网络为 2002:10::0/64, 网关地址为 2002:10::1。

```
[DHCPv6 server] ipv6 dhcp pool vlan 102
```

```
[DHCPv6 server-dhcp6-pool-vlan300] network 2002:10::0 64
```

```
[DHCPv6 server-dhcp6-pool-vlan300] gateway-list 2002:10::1
```

```
[DHCPv6 server-dhcp6-pool-vlan300] quit
```

### 3.4.5 AAA server 的配置



#### 说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0(E0202)、iMC UAM 5.0(E0202)），说明 AAA server 的基本配置。

# 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置认证、计费共享密钥为 123456789，其它保持缺省配置；
- 选择或手工增加接入设备，添加 IPv6 地址为 2000:10::10 和 2001:10::11 的接入设备。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 帮助

接入配置

认证端口 \*

1812

计费端口 \*

1813

组网方式

不启用混合组网

业务类型

LAN接入业务

接入设备类型

H3C(General)

接入设备分组

无

共享密钥 \*

\*\*\*\*\*

确认共享密钥 \*

\*\*\*\*\*

业务分组

未分组

设备列表

选择

手工增加

全部清除

| 设备名称 | 设备IP地址                             | 设备型号 | 备注 | 删除 |
|------|------------------------------------|------|----|----|
|      | 2001:0010:0000:0000:0000:0000:0011 |      |    | 删除 |
|      | 2000:0010:0000:0000:0000:0000:0010 |      |    | 删除 |

共有2条记录。

确定

取消

# 增加接入策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击<增加>按钮，进入增加接入策略页面。

- 设置接入策略名为 office；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证。

图3 增加接入策略页面

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略 帮助

基本信息

接入策略名 \*

office

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☐ 不启用 ☒ EAP证书认证 ☐ WAP证书认证

认证证书类型

EAP-PEAP认证

认证证书子类型

MS-CHAPV2认证

下发VLAN

下发用户组

☐ 下发User Profile

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

# 增加接入服务。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 设置服务名为 office；
- 选择缺省接入策略为 office，其他保持缺省配置。

图4 增加接入服务页面

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

帮助

基本信息

服务名 \*

office

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

office ?

缺省安全策略 \*

不使用

缺省内网外联配置 \*

不使用

缺省私有属性下发策略 \*

不使用 ?

缺省BYOD页面 \*

PC - 缺省页面 PC

服务描述

☒ 可申请 ?

☐ Portal无感知认证 ?

接入场景列表

增加

| 名称          | 接入策略 | 安全策略 | 私有属性下发策略 | 内网外联配置 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|------|----------|--------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |      |          |        |        |     |    |    |

确定

取消

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 单击<增加用户>添加用户 office，证件号码 123456；
- 添加帐号名为 office，密码为 123456；
- 选中刚才配置的服务 office。

图5 增加接入用户

用户姓名 \*

office

选择

增加用户

帐号名 \*

office

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                        | 服务后缀 | 缺省安全策略  | 状态  | 分配IP地址 |
|--------------------------------------------|------|---------|-----|--------|
| <input type="checkbox"/> 802.1x            |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> 8705-eap          |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> l4166             |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> lw_802.1x         |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> mpc_ead           |      | mpc_ead | 可申请 |        |
| <input type="checkbox"/> mpc_peap          |      | 不使用     | 可申请 |        |
| <input checked="" type="checkbox"/> office |      | 不使用     | 可申请 |        |

3.5 验证配置

# 客户端首先从 AC 1 下连接的 officeap1 的 VLAN 300 上线。通过 display wlan client verbose 命令可以看到客户端的详细信息。

```
[AC1] display wlan client verbose
Total Number of Clients          : 1
```

# Client Information

```

-----
MAC Address           : 0015-00ef-ac23
User Name             : office
IP Address            : 2002:10::2
AID                   : 1
AP Name               : officeap1
Radio Id              : 2
Antenna Id            : 0
Service Template Number : 1
SSID                  : service
BSSID                 : c8cb-b8f1-f6d0
Port                  : WLAN-DBSS1:1
VLAN                  : 300
State                 : Running
Power Save Mode       : Active
Wireless Mode         : 11g
QoS Mode              : WMM
Listen Interval (Beacon Interval) : 10
RSSI                  : 42
Rx/Tx Rate            : 48/36
Client Type           : WPA2(RSN)
Authentication Method : Open System
Authentication Mode    : Central
AKM Method             : Dot1X
4-Way Handshake State : PTKINITDONE
Group Key State        : IDLE
Encryption Cipher      : AES-CCMP
Roam Status           : Normal
Roam Count             : 0
Up Time (hh:mm:ss)    : 00:00:51
-----

```

# 通过 **display wlan mobility-group** 命令可以查看 IACTP 隧道信息。

```
[AC1] display wlan mobility-group
```

## Mobility Group Information

```

-----
Group Name           : office
Source IP Address    : 2000:10::10
Authentication Method : MD5
-----

```

## Member Information

```

-----
IPv6-address      State      Interface
-----
2001:10::11      Run          WLAN-Tunnel2
-----

```

```
[AC2] display wlan mobility-group
```

## Mobility Group Information

```

-----
Group Name           : office
Source IP Address    : 2001:10::11
Authentication Method : MD5
-----

```

#### Member Information

```

-----
IPv6-address      State      Interface
-----
2000:10::10      Run          WLAN-Tunnel2
-----

```

# 当客户端从 AC 1 下连接的 AP 1 漫游至 AC 2 下连接的 AP 2 上时，客户端信息同步到 AC 2，客户端不需要重新进行认证，客户端初始 VLAN 300 也被同步过来。通过 **display wlan client verbose** 命令在 AC 2 上显示客户端进行 AC 间漫游，信息如下：

```
[AC2] display wlan client verbose
```

```
Total Number of Clients      : 1
```

#### Client Information

```

-----
MAC Address           : 0015-00ef-ac23
User Name             : office
IP Address            : 2002:10::2
AID                   : 2
AP Name               : officeap2
Radio Id              : 2
Antenna Id            : 0
Service Template Number : 1
SSID                 : service
BSSID                : 0023-8930-9010
Port                 : WLAN-DBSS1:1
VLAN                 : 300
State                : Running
Power Save Mode       : Active
Wireless Mode         : 11g
QoS Mode              : WMM
Listen Interval (Beacon Interval) : 10
RSSI                  : 42
Rx/Tx Rate            : 48/36
Client Type           : WPA2(RSN)
Authentication Method : Open System
Authentication Mode    : Central
AKM Method            : Dot1X
4-Way Handshake State : PTKINITDONE
Group Key State        : IDLE
Encryption Cipher      : AES-CCMP
Roam Status           : Inter-AC roam association
Roam Count             : 1
Up Time (hh:mm:ss)    : 00:17:51
-----

```



# AC 1 上查询客户端漫游追踪信息，显示 Client 当前已经漫游至 AC 2:

```
[AC1] display wlan client roam-track mac-address 0015-00ef-ac23
```

| BSSID          | Online-time(d:h:m:s) | AC-IP-address         |
|----------------|----------------------|-----------------------|
| 0023-8930-9010 | 0000:00:21:19        | 2001:10::11           |
| c8cb-b8f1-f6d0 | 0000:00:19:14        | 2000:10::10 (HOME AC) |

## 3.6 配置文件

- AC 1:

```
#
port-security enable
#
dot1x authentication-method eap
#
vlan 101
#
vlan 200
#
vlan 300
#
radius scheme office
primary authentication ipv6 3000::1
primary accounting ipv6 3000::1
key authentication cipher $c$3$SjWMEAjbTjqCC9+XHRLYhNZOSJ6bBN/7K3HBEA==
key accounting cipher $c$3$Oj5WtaBGNaZb9s+R0Y/z0yKMG4fZcS0LuOUeOw==
user-name-format without-domain
nas-ip ipv6 2000:10::10
#
domain office
authentication lan-access radius-scheme office
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 1
cipher-suite tkip
cipher-suite ccmp
security-ie rsn
security-ie wpa
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
```

```

port trunk permit vlan 101 200 300
#
interface Vlan-interface101
  ipv6 address 2000:10::10/64
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
  port-security port-mode userlogin-secure-ext
  port-security tx-key-type 11key
  undo dot1x handshake
  dot1x mandatory-domain office
  undo dot1x multicast-trigger
#
wlan ap officeap1 model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
  service-template 1 vlan-id 300
  radio enable
#
wlan mobility-group office
  member ipv6 2000:10::10
  source ipv6 2001:10::11
  authentication-mode MD5 cipher $c$3$0ltSGsSqV3ls4QJM7n6PXHtOFKFDS c3d9Q==
  mobility-group enable
#
ipv6 route-static 0::0 64 2000:10::11
#

```

## - AC 2:

```

#
port-security enable
#
dot1x authentication-method eap
#
vlan 102
#
vlan 200
#
vlan 300
#
radius scheme office
  primary authentication ipv6 3000::1
  primary accounting ipv6 3000::1
  key authentication cipher $c$3$SjWMEAjBTjqCC9+XhRLYhNZOSJ6bBN/7K3HBEA==

```

```

key accounting cipher $c$3$Oj5WtaBGNaZb9s+R0Y/z0yKMG4fZcS0LuOUeOw==
user-name-format without-domain
nas-ip ipv6 2000:10::10
#
domain office
    authentication lan-access radius-scheme office
    access-limit disable
    state active
    idle-cut disable
    self-service-url disable
#
wlan service-template 1 crypto
    ssid service
    bind WLAN-ESS 1
    cipher-suite tkip
    cipher-suite ccmp
    security-ie rsn
    security-ie wpa
    service-template enable
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 102 200 300
#
interface Vlan-interface102
    ipv6 address 2001:10::11/64
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
    port-security port-mode userlogin-secure-ext
    port-security tx-key-type 11key
    undo dot1x handshake
    dot1x mandatory-domain office
    undo dot1x multicast-trigger
#
wlan ap officeap2 model WA2620E-AGN id 1
    serial-id 21023529G007C000021
    radio 1
    radio 2
        service-template 1 vlan-id 300
    radio enable
#
wlan mobility-group office
    member ip 2000:10::10

```

```

source ipv6 2001:10::11
authentication-mode MD5 cipher $c$3$0ltSGsSqV3ls4QJM7n6PXHtOFKFDSc3d9Q==
mobility-group enable
#
ipv6 route-static 0::0 64 2001:10::10
#

```

- **Switch:**

```

#
vlan 101 to 102
#
vlan 300
#
interface Vlan-interface101
    ipv6 address 2000:10::11/64
#
interface Vlan-interface102
    ipv6 address 2001:10::10/64
#
interface GigabitEthernet1/0/1
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan 1 101 300
    port trunk pvid vlan 101
#
interface GigabitEthernet1/0/2
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan 1 102 300
    port trunk pvid vlan 102
#
interface GigabitEthernet1/0/3
    port link-mode bridge
    port access vlan 101
    poe enable
#
interface GigabitEthernet1/0/4
    port link-mode bridge
    port access vlan 102
    poe enable
#
#
interface GigabitEthernet1/0/5
    port link-mode route
    ipv6 address 3000::3/64

```

- **DHCP server:**

```

#
vlan 101 to 102

```

```

#
vlan 300
#
ipv6 dhcp pool vlan101
    network 2000:10::0 64
#
ipv6 dhcp pool vlan102
    network 2001:10::0 64
#
ipv6 dhcp pool vlan300
    network 2002:10::0 64
#
interface Vlan-interface101
    ipv6 dhcp server apply pool 101
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    ipv6 address 2000:10::1/64
#
interface Vlan-interface102
    ipv6 dhcp server apply pool 102
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    ipv6 address 2001:10::1/64
#
interface Vlan-interface300
    ipv6 dhcp server apply pool 300
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    ipv6 address 2002:10::1/64
#
interface GigabitEthernet1/0/1
    port link-mode route
    ipv6 address 3000::2/64
#
ipv6
#
    ipv6 dhcpv6 server enable
#
ipv6 route-static 0::0 64 3000::2
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# AP 和无线用户属于不同 VLAN 的无线接入典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤.....          | 1 |
| 3.3.1 AC 的配置 .....     | 1 |
| 3.3.2 Switch 的配置 ..... | 3 |
| 3.4 验证配置 .....         | 4 |
| 3.5 配置文件 .....         | 5 |
| 4 相关资料 .....           | 6 |

# 1 简介

本文档介绍了当 AP 和无线用户属于不同 VLAN 时的无线接入配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

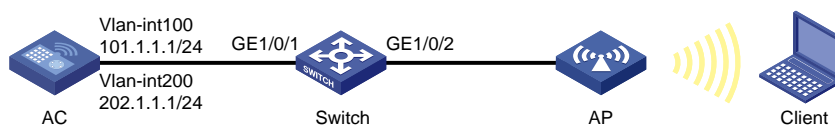
本文档假设您已了解 WLAN 接入特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，通过将 AP 和无线用户划分在不同的 VLAN 中，以保证 AC 和 AP 之间的通信不受其他局域网中数据报文的干扰，进而增强 AP 和 AC 通信的安全性和稳健性，更好的统一管理有线网络和无线网络。AC 作为 DHCP 服务器为 AP 分配 101.1.1.0/24 网段的 IP 地址，为 Client 分配 202.1.1.0/24 网段的 IP 地址。

图1 AP 和无线用户属于不同 VLAN 配置组网图



### 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.3 配置步骤

#### 3.3.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址 101.1.1.1/24。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
```



```

[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 101.1.1.1 24
[AC-Vlan-interface100] quit
# 创建 VLAN 200, 作为 ESS 接口的缺省 VLAN, 同时作为 Client 接入的业务 VLAN, 并配置 VLAN
接口 200 的 IP 地址为 202.1.1.1/24。
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 202.1.1.1 24
[AC-Vlan-interface200] quit
# 配置 GigabitEthernet 1/0/1 接口的链路类型为 Trunk, 允许 VLAN 100 和 VLAN 200 的报文通过。
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk vlan 100 200
[AC-GigabitEthernet1/0/1] quit
(2) 配置 DHCP 服务
# 使能 DHCP 服务。
[AC] dhcp enable
# 创建名称为 for_aps 的 DHCP 普通模式地址池, 为 AP 分配 101.1.1.0/24 网段的 IP 地址, 网关地
址为 101.1.1.1。
[AC] dhcp server ip-pool for_aps
[AC-dhcp-pool-for_aps] network 101.1.1.0 mask 255.255.255.0
[AC-dhcp-pool-for_aps] gateway-list 101.1.1.1
[AC-dhcp-pool-for_aps] quit
# 创建名称为 for_clients 的 DHCP 普通模式地址池, 为 Client 分配 202.1.1.0/24 网段的 IP 地址,
网关地址为 202.1.1.1。
[AC] dhcp server ip-pool for_clients
[AC-dhcp-pool-for_clients] network 202.1.1.0 24
[AC-dhcp-pool-for_clients] gateway-list 202.1.1.1
[AC-dhcp-pool-for_clients] quit
(3) 配置 WLAN-ESS 接口
# 创建编号为 1 的 WLAN-ESS 接口。
[AC] interface wlan-ess 1
# 配置端口的链路类型为 hybrid。
[AC-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 200, 禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
# 在 Hybrid 端口上使能 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
(4) 配置服务模板
# 创建 clear 类型的服务模板 1。

```

```
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID（服务模板的标识）为 market_department。
[AC-wlan-st-1] ssid market_department
# 将 WLAN-ESS 1 接口绑定到服务模板。
[AC-wlan-st-1] bind wlan-ess 1
# 设置无线客户端接入该无线服务（SSID）的认证方式为开放式系统认证。
[AC-wlan-st-1] authentication-method open-system
# 使能服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### (5) 配置 AP

```
# 创建 AP 管理模板，其名称为 officeap，型号名称这里选择 WA2620E-AGN。
[AC] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 设置 radio 2 的射频类型为 802.11gn。
[AC-wlan-ap-officeap] radio 2 type dot11gn
# 将服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-officeap-radio-2] service-template 1
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] return
```

## 3.3.2 Switch 的配置

```
# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 200 为无线用户接入的 VLAN。
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 200 通过。
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access，当前 Access 口允许 VLAN 100 通过。
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

### 3.4 验证配置

- (1) 在 AC 上通过 **display wlan ap all** 命令查看 AP 状态，确认 AP 可以和 AC 处于连接状态，并且 WLAN-ESS 1 接口处于 UP 状态。

```
<AC> display wlan ap all
Total Number of APs configured          : 1
Total Number of configured APs connected : 1
Total Number of auto APs connected      : 0

AP Profiles
State : I = Idle,   J = Join, JA = JoinAck,   IL = ImageLoad
       C = Config, R = Run,   KU = KeyUpdate, KC = KeyCfm

-----
AP Name                State   Model                Serial-ID
-----
officeap               R/M   WA2620E-AGN          21023529G007C000020
-----
```

```
<AC> display interface brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing

Interface          Link Protocol Main IP          Description
M-GE1/0/0          DOWN DOWN          --
NULL0              UP    UP(s)           --
Vlan1              UP    UP              --
Vlan100            UP    UP              101.1.1.1
Vlan200            UP    UP              202.1.1.1
```

```
The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid

Interface          Link Speed    Duplex Type PVID Description
GE1/0/1            UP   1000M(a)F    T     1
GE1/0/2            UP   1000M(a)F    T     1
WLAN-ESS1          UP   --          --    H     200
WLAN-DBSS1:1       UP   --          --    H     200
```

- (2) 在 Client 上验证，可以连接 SSID 为 “market\_department” 的无线网络。

# Client 可以和 Server 通信。

```
C:\> ping 202.1.1.1
```

Pinging 202.1.1.1 with 32 bytes of data:

Reply from 202.1.1.1: bytes=32 time=13ms TTL=128

Reply from 202.1.1.1: bytes=32 time=2ms TTL=128

Reply from 202.1.1.1: bytes=32 time=39ms TTL=128

Reply from 202.1.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 202.1.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 39ms, Average = 13ms

## 3.5 配置文件

- AC:

```
#
vlan 100
#
vlan 200
#
dhcp server ip-pool for_aps
    network 101.1.1.0 mask 255.255.255.0
    gateway-list 101.1.1.1
#
dhcp server ip-pool for_clients
    network 202.1.1.0 mask 255.255.255.0
    gateway-list 202.1.1.1
#
wlan service-template 1 clear
    ssid market_department
    bind WLAN-ESS 1
    authentication-method open-system
    service-template enable
#
interface Vlan-interface100
    ip address 101.1.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 202.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
```

```

port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN
serial-id 21023529G007C000020
radio 2 type dot11gn
service-template 1
radio enable
#
dhcp enable
#
• Switch:
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“三层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“三层技术命令参考”。

# AP 通过 DNS 获取 AC 列表注册典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项.....        | 1 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 DNS 服务器的配置.....  | 2 |
| 3.4.2 AC 的配置 .....     | 3 |
| 3.4.3 Switch 的配置 ..... | 5 |
| 3.5 验证配置 .....         | 6 |
| 3.6 配置文件 .....         | 7 |
| 4 相关资料 .....           | 8 |

# 1 简介

本文档介绍了 AP 通过 DNS 方式获取 AC 的 IP 地址并完成注册的配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

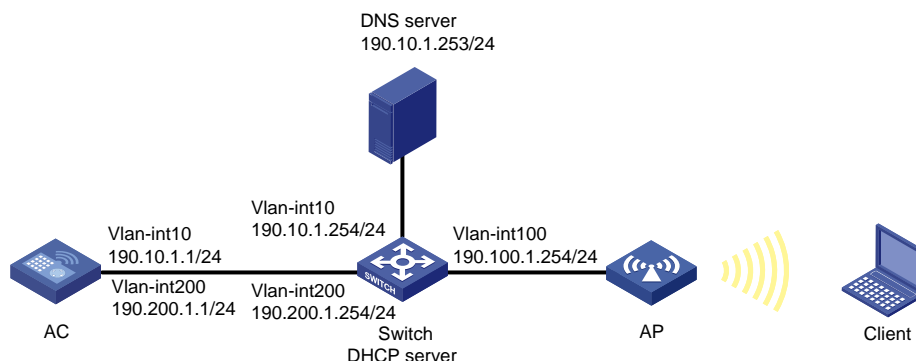
本文档假设您已了解 WLAN 接入和 DNS 特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AP 与 AC 之间跨越三层网络连接，现要求：通过配置 AP 通过 DNS 方式获取 AC 的 IP 地址，从而能与 AC 之间建立隧道连接，为无线用户提供 WLAN 接入服务的功能。

图1 AP 通过 DNS 方式获取 AC 地址注册组网图



### 3.2 配置思路

在 Switch 上配置 DHCP 服务，为 AP 分配 IP 地址、AC 域名、DNS 服务器地址，使 AP 可以通过解析 DNS 服务器中的 AC 域名记录获取 AC 列表。

### 3.3 配置注意事项

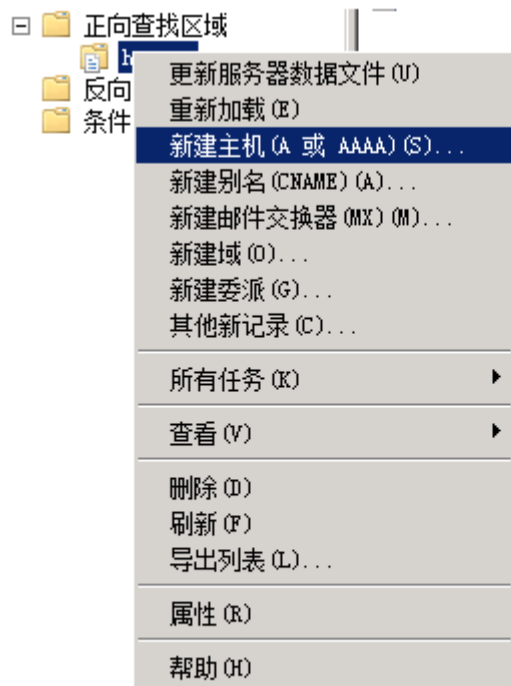
配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。



## 3.4 配置步骤

### 3.4.1 DNS 服务器的配置

# 如下图所示，在 DNS server 上创建 AC 对应的域名，在该域名下建立 AC 解析项（AC 的主机名为 pn）。



# 在弹出的“新建主机”对话框中输入主机名称为 pn，IP 地址为 190.10.1.1，点击<添加主机 (H)> 按钮，完成主机 pn.h3c.com 的创建。

**新建主机**

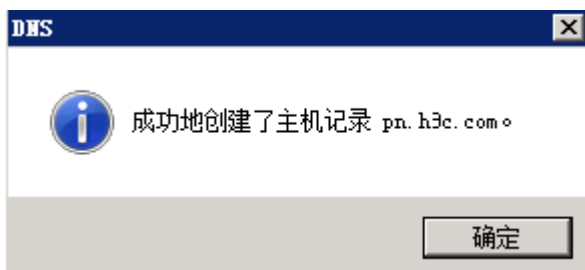
名称 (如果为空则使用其父域名称) (N):  
pn

完全限定的域名 (FQDN):  
pn.h3c.com

IP 地址 (P):  
190.10.1.1

☐ 创建相关的指针 (PTR) 记录 (C)

添加主机 (O)    取消



### 3.4.2 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 10 和 VLAN 200。其中 VLAN10 作为 AC 和 DNS 之间连接的 VLAN，VLAN 200 作为 WLAN-ESS 接口使用的 VLAN。

```
<AC> system-view
[AC] vlan 10
[AC-vlan10] quit
[AC] vlan 200
[AC-vlan200] quit
```

# 配置 VLAN 10 的 IP 地址为 190.10.1.1/24。

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 190.10.1.1 24
[AC-Vlan-interface10] quit
```

# 配置 VLAN 200 的接口 IP 地址为 190.200.1.1/24。

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 190.200.1.1 24
[AC-Vlan-interface200] quit
```

# 配置默认路由，使 AC 和 AP 可以跨三层通信。

```
[AC] ip route-static 0.0.0.0 0 190.10.1.254
```

# 配置 AC 的连接交换机的 GigabitEthernet1/0/1 接口的属性为 Trunk，禁止 VLAN1 通过，允许 VLAN 10 和 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
```

```
[AC-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[AC-GigabitEthernet1/0/1] port trunk permit vlan 10 200
```

```
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
```

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

## (2) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

## (3) 配置射频接口并绑定服务模板

# 创建 AP 的管理模板，名称为 officeap，型号名称这里选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 officeap 的序列号为 21023529G007C000020

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联。

```
[AC-wlan-ap-officeap-radio-2] service-template 1
```

# 使能 officeap 的 radio 2。

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

```
[AC-wlan-ap-officeap] quit
```

### 3.4.3 Switch 的配置

# 创建 VLAN 10、VLAN 100 和 VLAN 200，其中 VLAN10 用于连接 DNS 服务器，VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 10、100、200 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 10 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DNS 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN10 通过。

```
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 10
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 VLAN 10 的接口地址为 190.10.1.254/24

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 190.10.1.254 24
[Switch-Vlan-interface10] quit
```

# 配置 VLAN 100 的接口地址为 190.100.1.254/24

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 190.100.1.254 24
[Switch-Vlan-interface100] quit
```

# 配置 VLAN 200 的接口地址为 128.200.1.254/24

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 128.200.1.254 24
[Switch-Vlan-interface200] quit
```

# 配置 Switch 使能 DHCP 服务。

```
[Switch] dhcp enable
```

# 创建名为 **vlan100** 的 DHCP 地址池，配置地址池范围为 190.100.1.0~190.100.1.250，网关地址为 190.100.1.254，为 AP 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan100 extended
[Switch-dhcp-pool-vlan100] network ip range 190.100.1.0 190.100.1.250
[Switch-dhcp-pool-vlan100] network mask 255.255.255.0
[Switch-dhcp-pool-vlan100] gateway-list 190.100.1.254
[Switch-dhcp-pool-vlan100] dns-list 190.10.1.253
[Switch-dhcp-pool-vlan100] domain-name h3c.com
[Switch-dhcp-pool-vlan100] quit
```

# 创建名为 **vlan200** 的 DHCP 地址池，配置地址池范围为 190.200.1.0~190.200.1.250，网关地址为 190.200.1.254，为 Client 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan200 extended
[Switch-dhcp-pool-vlan300] network ip range 190.200.1.0 190.200.1.250
[Switch-dhcp-pool-vlan300] network mask 255.255.255.0
[Switch-dhcp-pool-vlan300] gateway-list 190.200.1.254
[Switch-dhcp-pool-vlan300] quit
```

### 3.5 验证配置

# 通过命令 **display wlan ap all** 可以在 AC 上查看到 AP 已经成功注册。

```
[AC] display wlan ap all
Total Number of APs configured          : 1
Total Number of configured APs connected : 1
Total Number of auto APs connected      : 0

                        AP Profiles
State : I = Idle,   J = Join, JA = JoinAck,   IL = ImageLoad
       C = Config, R = Run,   KU = KeyUpdate, KC = KeyCfm
       M = Master, B = Backup

-----
AP Name                               State Model                Serial-ID
-----
officeap                             R/M    WA2620E-AGN             21023529G007C000020
-----
```

# 通过命令 **display wlan client** 可以看到在线的无线客户端。

```
[AC] display wlan client
Total Number of Clients          : 1

                        Client Information
SSID: service

-----
MAC Address    User Name      APID/RID IP Address                VLAN
-----
acf1-df11-a565  -NA-                1 /2    190.200.1.2                200
-----
```

# AC 可以 ping 通无线客户端。

```
[AC] ping 190.200.1.2
PING 190.200.1.2: 56 data bytes, press CTRL_C to break
Reply from 190.200.1.2: bytes=56 Sequence=0 ttl=63 time=2 ms
```

```

Reply from 190.200.1.2: bytes=56 Sequence=1 ttl=63 time=4 ms
Reply from 190.200.1.2: bytes=56 Sequence=2 ttl=63 time=2 ms
Reply from 190.200.1.2: bytes=56 Sequence=3 ttl=63 time=36 ms
Reply from 190.200.1.2: bytes=56 Sequence=4 ttl=63 time=4 ms

--- 190.200.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 2/9/36 ms

```

## 3.6 配置文件

```

• AC

#
vlan 10
#
vlan 200
#
wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable
#
interface Vlan-interface10
  ip address 190.10.1.1 255.255.255.0
#
interface Vlan-interface200
  ip address 190.200.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 10 200
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
  service-template 1
  radio enable

```

```

#
ip route-static 0.0.0.0 0.0.0.0 190.10.1.254
#
•   Switch
#
vlan 10
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100 extended
    network ip range 190.100.1.0 192.100.1.250
    network mask 255.255.255.0
    dns-list 190.10.1.253
    domain-name h3c.com
    gateway-list 190.100.1.254
#
dhcp server ip-pool vlan200 extended
    network ip range 190.200.1.0 190.200.1.250
    network mask 255.255.255.0
    gateway-list 190.200.1.254
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 10 100 200
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
    port link-mode bridge
    port access vlan 100
    poe enable
#
interface Vlan-interface10
    ip address 190.10.1.254 255.255.0.0
#
interface Vlan-interface100
    ip address 190.100.1.254 255.255.255.0
#
interface Vlan-interface300
    ip address 190.200.1.254 255.255.255.0
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“三层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“三层技术命令参考”。

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。



# AP 自动注册典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置步骤 .....         | 1 |
| 3.2.1 AC 的配置 .....     | 1 |
| 3.2.2 Switch 的配置 ..... | 2 |
| 3.3 验证配置 .....         | 3 |
| 3.4 配置文件 .....         | 3 |
| 4 相关资料 .....           | 4 |

# 1 简介

本文档介绍 AP 自动注册配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

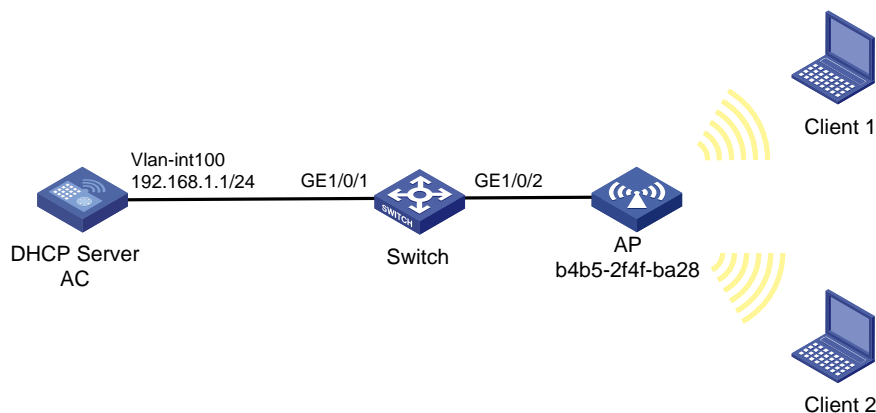
本文档假设您已了解自动 AP 功能。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址，现要求使用 AP 自动注册功能，实现 AP 与 AC 自动关联，并且在关联后将 AP 转化为固化 AP。

图1 AP 自动注册配置举例组网图



### 3.2 配置步骤

#### 3.2.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
```

```
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.1 24
[AC-Vlan-interface100] quit
```

## (2) 配置 DHCP 功能

# 全局下使能 DHCP 功能。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 1 为 AP 和 Client 动态分配的网段为 192.168.1.0/24, 网关地址为 192.168.1.1。

```
[AC] dhcp server ip-pool 1
[AC-dhcp-pool-1] network 192.168.1.0 24
[AC-dhcp-pool-1] gateway-list 192.168.1.1
[AC-dhcp-pool-1] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk, 当前 Trunk 口的 PVID 为 100, 禁止 VLAN1 通过, 允许 VLAN 100 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100
[AC-GigabitEthernet1/0/1] quit
```

## (3) 配置 AP 自动注册功能

# 开启自动 AP 功能。

```
[AC] wlan auto-ap enable
```

# 创建一个 AP 管理模板, 其名称为 officeap1, 型号名称为 WA2620E-AGN。

```
[AC] wlan ap officeap1 model WA2620E-AGN
```

# 设置自动查找 AP 序列号。

```
[AC-wlan-ap-officeap1] serial-id auto
[AC-wlan-ap-officeap1] quit
```

# 将所有自动 AP 转换为固化 AP, 但名称保持不变。

```
[AC] wlan auto-ap persistent all
```

## 3.2.2 Switch 的配置

# 创建 VLAN 100, 用于转发 AC 和 AP 间 LWAPP 隧道内的流量。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk, 禁止 VLAN 1 通过, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 当前 Access 口允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

### 3.3 验证配置

# 按照如上配置, AC 与 AP 可以进行关联。通过 **display wlan ap all** 命令看到 AP 的状态为 Run。

```
[AC] display wlan ap all
```

```
Total Number of APs configured          : 1
Total Number of configured APs connected : 0
Total Number of auto APs connected       : 1
   AP Profiles
```

| AP Name        | APID | State | Model       | Serial-ID           |
|----------------|------|-------|-------------|---------------------|
| officeap1      | 1    | Idle  | WA2620E-AGN | auto                |
| b4b5-2f4f-ba28 | 2    | Run   | WA2620E-AGN | 21023529G007C000020 |

### 3.4 配置文件

- AC

```
#
vlan 100
#
wlan auto-ap enable
#
dhcp server ip-pool 1
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.1
#
interface Vlan-interface100
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk pvid vlan 100
port trunk permit vlan 100
#
wlan ap officeap1 model WA2620E-AGN
serial-id auto
```

```
radio 1
#
dhcp enable
#
• Switch
#
vlan 100
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# H3C 无线控制器 IPv6 三层注册典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                         |   |
|-------------------------|---|
| 1 简介.....               | 1 |
| 2 配置前提 .....            | 1 |
| 3 IPv6 三层网络注册配置举例 ..... | 1 |
| 3.1 组网需求 .....          | 1 |
| 3.2 配置思路 .....          | 1 |
| 3.3 配置注意事项.....         | 2 |
| 3.4 配置步骤 .....          | 2 |
| 3.4.1 配置 AC.....        | 2 |
| 3.4.2 配置 L3 switch..... | 3 |
| 3.5 验证配置 .....          | 5 |
| 3.6 配置文件 .....          | 6 |
| 4 相关资料 .....            | 8 |



# 1 简介

本文档介绍 AP 与 AC 间通过三层网络完成注册的配置举例。

## 2 配置前提

本文档适用于使用 Comware V5 软件版本的无线控制器和接入点产品，不严格与具体硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IPv6 基础与 WLAN 接入相关特性。

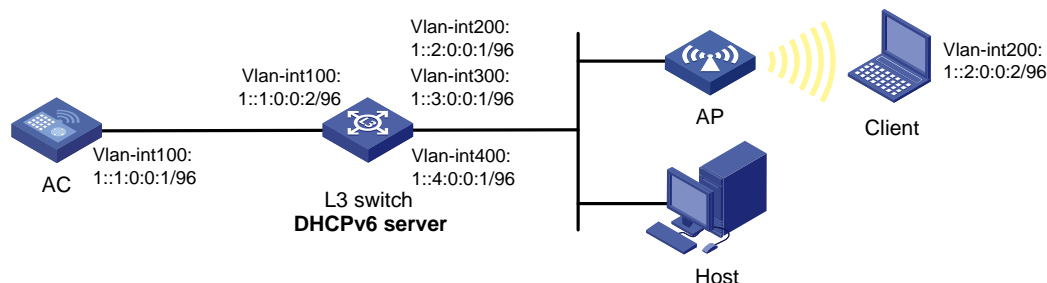
## 3 IPv6 三层网络注册配置举例

### 3.1 组网需求

如图 1 所示，集中式转发架构下，无线客户端 Client、有线客户端 Host 通过 L3 switch 与 AC 相连，L3 switch 做 DHCPv6 server 为 AP、Client 和 Host 分配 IPv6 地址。要实现无线客户端 Client 通过 AP 连接到 AC 上，并能与有线客户端 Host 互相访问，具体要求如下：

- 无线客户端 Client 通过 VLAN 200 接入网络，有线客户端 Host 通过 VLAN 300 接入网络；
- AC 属于 VLAN 100，AP 属于 VLAN 400，AC 和 AP 之间跨三层网络建立连接。

图1 Fit AP 通过三层网络注册到 AC 配置举例组网图



### 3.2 配置思路

- 在 L3 switch 上配置 DHCPv6 server 服务，使 AP、无线客户端 Client 和有线客户端 Host 都能通过 DHCPv6 server 自动获取 IPv6 地址。
- 在 L3 switch 和 AC 上配置到达对端网段的静态路由。
- 在 AC 上配置无线服务，确保 Client 可以通过配置的无线服务接入网络，并访问 Host。

### 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 配置 L3 switch 和 AP 相连的接口禁止 VLAN 1 报文通过，以防止 VLAN 1 内报文过多。

### 3.4 配置步骤

#### 3.4.1 配置 AC

##### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。AC 将使用该接口的 IPv6 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface100
[AC-Vlan-interface100] ipv6 address 1::1:0:0:1/96
[AC-Vlan-interface100] quit
```

# 创建 VLAN 101 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 101
[AC-vlan101] quit
```

# 创建 VLAN 200，AC 需要使用该 VLAN 转发无线客户端数据报文。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 配置 AC 和 L3 switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100、VLAN 101、VLAN 200 和 VLAN 400 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 101 200 400
[AC-GigabitEthernet1/0/1] quit
```

##### (2) 配置三层路由

# 配置 AC 到 1::2:0:0:0 网段的静态路由，指定下一跳的 IP 地址为 1::1:0:0:2。

```
[AC] ipv6 route-static 1::4:0:0:0 96 1::1:0:0:2
```

##### (3) 配置 WLAN-ESS 接口

# 创建 WLAN-ESS1 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 101，禁止 VLAN 1 通过并且允许 VLAN 100、VLAN 200 和 VLAN 400 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 100 200 400 untagged
```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 101
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

#### (4) 配置无线服务

# 创建 **clear** 类型的服务模板 1，并进入服务模板视图。

```
[AC] wlan service-template 1 clear
```

# 配置 SSID 为 **service**。

```
[AC-wlan-st-1] ssid service
```

# 将 **WLAN-ESS1** 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用服务模板。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

#### (5) 配置射频接口并绑定服务模板

# 创建 **AP** 的管理模板，名称为 **officeap**，型号名称为 **WA2620E-AGN**。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 **officeap** 的序列号为 **21023529G007C000020**。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 **AP** 的 **Radio 1** 视图，并将服务模板 1 与射频 **Radio 1** 关联，同时设置绑定到该射频的 **VLAN** 为 **VLAN 200**。

```
[AC-wlan-ap-officeap] radio 1
```

```
[AC-wlan-ap-officeap-radio-1] service-template 1 vlan-id 200
```

# 使能 **officeap** 的 **Radio 1**。

```
[AC-wlan-ap-officeap-radio-1] radio enable
```

```
[AC-wlan-ap-officeap-radio-1] return
```

### 3.4.2 配置 L3 switch

#### (1) 配置 L3 switch 的接口

# 创建 **VLAN 400** 和 **VLAN 100**，并配置 **IPv6** 地址，用于转发 **AC** 和 **AP** 间的 **LWAPP** 隧道内的流量。

```
<L3 switch> system-view
```

```
[L3 switch] vlan 100
```

```
[L3 switch-vlan100] quit
```

```
[L3 switch] interface vlan-interface 100
```

```
[L3 switch-Vlan-interface100] ipv6 address 1::1:0:0:2/96
```

```
[L3 switch-Vlan-interface100] quit
```

```
[L3 switch] vlan 400
```

```
[L3 switch-vlan400] quit
```

```
[L3 switch] interface vlan-interface 400
```

```
[L3 switch-Vlan-interface400] ipv6 address 1::4:0:0:1/96
```

```
[L3 switch-Vlan-interface400] quit
```

# 创建 **VLAN 200**，并为该接口配置 **IPv6** 地址。**Client** 使用该 **VLAN** 接入无线网络。

```
[L3 switch] vlan 200
```

```
[L3 switch-vlan200] quit
[L3 switch] interface vlan-interface 200
[L3 switch-Vlan-interface200] ipv6 address 1::2:0:0:1/96
[L3 switch-Vlan-interface200] quit
```

# 创建 VLAN 300，并为该接口配置 IPv6 地址。Host 使用该 VLAN 与 AC 建立连接。

```
[L3 switch] vlan 300
[L3 switch-vlan300] quit
[L3 switch] interface vlan-interface 300
[L3 switch-Vlan-interface300] ipv6 address 1::3:0:0:1/96
[L3 switch-Vlan-interface300] quit
```

# 配置 L3 switch 和 AC 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN100、VLAN 101、VLAN 200 和 VLAN 400 通过。

```
[L3 switch] interface gigabitEthernet 1/0/1
[L3 switch-GigabitEthernet1/0/1] port link-type trunk
[L3 switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[L3 switch-GigabitEthernet1/0/1] port trunk permit vlan 100 101 200 400
[L3 switch-GigabitEthernet1/0/1] quit
```

# 配置 L3 switch 和 AP 相连的接口 GigabitEthernet1/0/2 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 400 和 VLAN 200 通过，当前 Trunk 口的 PVID 为 400。

```
[L3 switch] interface gigabitEthernet 1/0/2
[L3 switch-GigabitEthernet1/0/2] port link-type trunk
[L3 switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[L3 switch-GigabitEthernet1/0/2] port trunk permit vlan 200 400
[L3 switch-GigabitEthernet1/0/2] port trunk pvid vlan 400
[L3 switch-GigabitEthernet1/0/2] quit
```

# 配置 L3 switch 和 Host 相连的接口 GigabitEthernet1/0/3 为 Access 类型，允许 VLAN 300 通过。

```
[L3 switch] interface gigabitEthernet 1/0/3
[L3 switch-GigabitEthernet1/0/3] port access vlan 300
[L3 switch-GigabitEthernet1/0/3] quit
```

## (2) 配置 DHCPv6 服务

# 开启 IPv6 报文转发及 DHCPv6 服务器功能。

```
[L3 switch] ipv6
[L3 switch] ipv6 dhcp server enable
```

# 配置 DHCPv6 地址池 1，为 1::2:0:0:0/96 网段的客户端分配 IPv6 地址等参数。

```
[L3 switch] ipv6 dhcp pool 1
[L3 switch-dhcp6-pool-1] network 1::2:0:0:0/96
[L3 switch-dhcp6-pool-1] quit
```

# 配置 DHCPv6 地址池 2，为 1::3:0:0:0/96 网段的客户端分配 IPv6 地址等参数。

```
[L3 switch] ipv6 dhcp pool 2
[L3 switch-dhcp6-pool-2] network 1::3:0:0:0/96
[L3 switch-dhcp6-pool-2] quit
```

# 配置 DHCPv6 地址池 3，为 1::4:0:0:0/96 网段的 AP 分配 IPv6 地址等参数，并通过自定义选项的方式配置 option 52 的内容，为 AP 指定 AC 的 IPv6 地址 1::1:0:0:1。

```
[L3 switch] ipv6 dhcp pool 3
[L3 switch-dhcp6-pool-3] network 1::4:0:0:0/96
[L3 switch-dhcp6-pool-3] option 52 hex 0001000000000000000000000100000001
```

```
[L3 switch-dhcp6-pool-3] quit
# 配置接口 Vlan-interface200、Vlan-interface300 和 Vlan-interface400 工作在 DHCPv6 服务器模式，并分别引用地址池 1、2 和 3。
[L3 switch] interface vlan-interface 200
[L3 switch-Vlan-interface200] ipv6 dhcp server apply pool 1
[L3 switch-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[L3 switch-Vlan-interface200] ipv6 nd autoconfig other-flag
[L3 switch-Vlan-interface200] quit
[L3 switch] interface vlan-interface 300
[L3 switch-Vlan-interface300] ipv6 dhcp server apply pool 2
[L3 switch-Vlan-interface300] ipv6 nd autoconfig managed-address-flag
[L3 switch-Vlan-interface300] ipv6 nd autoconfig other-flag
[L3 switch-Vlan-interface300] quit
[L3 switch] interface vlan-interface 400
[L3 switch-Vlan-interface400] ipv6 dhcp server apply pool 3
[L3 switch-Vlan-interface400] ipv6 nd autoconfig managed-address-flag
[L3 switch-Vlan-interface400] ipv6 nd autoconfig other-flag
[L3 switch-Vlan-interface400] quit
```

## 3.5 验证配置

(1) 在 AC 上查看到 AP 注册信息

# 在 AC 上使用命令 **display wlan ap all** 查看 AP，可以看到 AP 的状态是 R/M，表明 AP 已经成功注册到 AC。

```
<AC> display wlan ap all
Total Number of APs configured          : 1
Total Number of configured APs connected : 1
Total Number of auto APs connected      : 0

AP Profiles
State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
       C = Config, R = Run, KU = KeyUpdate, KC = KeyCfm
       M = Master, B = Backup
```

| AP Name | State | Model       | Serial-ID           |
|---------|-------|-------------|---------------------|
| ap1     | R/M   | WA2620E-AGN | 21023529G007C000020 |

(2) 在 AC 上查看 Client 信息

# 在 AC 上使用命令 **display wlan client** 查看在线 Client，可以看到 Client 已经连接到 AP 的 radio1。

```
<AC> display wlan client
Total Number of Clients          : 1

Client Information
SSID: service
```

| MAC Address    | User Name | APID/RID | IP Address | VLAN |
|----------------|-----------|----------|------------|------|
| 000f-e265-6400 | -NA-      | 1/1      | 1::2:0:0:2 | 200  |

### (3) Host 与 Client 可以相互 ping 通

# Client 通过 DHCP server 获取到 IP 地址 1::2:0:0:2, 在 Host 上 ping Client 的 IPv6 地址可以 ping 通。同理, 在 Client 上 ping Host 的 IPv6 地址也能 ping 通, 不再赘述。

```
C:\Users\system32>ping 1::2:0:0:2 -t

Pinging 1::2:0:0:2 with 32 bytes of data:
Reply from 1::2:0:0:2: bytes=32 time=2470ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=2ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=1427ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=2ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=86ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=142ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=561ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=84ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=465ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=114ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=124ms TTL=63
Reply from 1::2:0:0:2: bytes=32 time=446ms TTL=63

Ping statistics for 1::2:0:0:2:
    Packets: Sent = 12, Received = 12, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2470ms, Average = 495ms
Control-C
^C
C:\Users\system32>
```

## 3.6 配置文件

- AC

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
    ipv6 address 1::1:0:0:1/96
#
interface Vlan-interface101
    ipv6 address 1::5:0:0:1/96
#
interface Vlan-interface200
    ipv6 nd snooping enable
#
wlan service-template 1 clear
    ssid service
    service-template enable
```

```

#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#
ipv6 route-static 1::4:0:0:0 96 1::1:0:0:2
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 100 200 400 untagged
port hybrid pvid vlan 201
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN
serial-id WA2620E-AGN
vlan 1
radio 1
radio enable
service-template 1 vlan 200
radio 2
#
•   L3 switch
#
vlan 100
#
vlan 101
#
vlan 200
#
vlan 300
#
vlan 400
#
ipv6 dhcp pool 1
network 1::2:0:0:0/96
#
ipv6 dhcp pool 2
network 1::3:0:0:0/96
#
ipv6 dhcp pool 3
network 1::4:0:0:0/96
option 52 hex 000100000000000000001000000000001
#
interface Vlan-interface100
ipv6 address 1::1:0:0:2/96
#

```

```

interface Vlan-interface200
  ipv6 dhcp server apply pool 1
  ipv6 address 1::2:0:0:1/96
  ipv6 nd autoconfig managed-address-flag
  ipv6 nd autoconfig other-flag
#
interface Vlan-interface300
  ipv6 dhcp server apply pool 2
  ipv6 address 1::3:0:0:1/96
  ipv6 nd autoconfig managed-address-flag
  ipv6 nd autoconfig other-flag
#
interface Vlan-interface400
  ipv6 dhcp server apply pool 3
  ipv6 address 1::4:0:0:1/96
  ipv6 nd autoconfig managed-address-flag
  ipv6 nd autoconfig other-flag
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200 400
#
interface GigabitEthernet1/0/2
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 200 400
  port trunk pvid vlan 400
#
interface GigabitEthernet1/0/3
  port access vlan 300
#
  ipv6
#
  ipv6 dhcp server enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“三层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“三层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。



# IPsec 加密 AC 与 AP 间隧道典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                 |   |
|-----------------|---|
| 1 简介.....       | 1 |
| 2 配置前提 .....    | 1 |
| 3 配置举例 .....    | 1 |
| 3.1 组网需求 .....  | 1 |
| 3.2 配置思路 .....  | 1 |
| 3.3 配置注意事项..... | 1 |
| 3.4 配置步骤 .....  | 2 |
| 3.5 验证配置 .....  | 4 |
| 3.6 配置文件 .....  | 5 |
| 4 相关资料 .....    | 7 |

# 1 简介

本文档介绍 IPsec 加密 AC 与 AP 间隧道的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

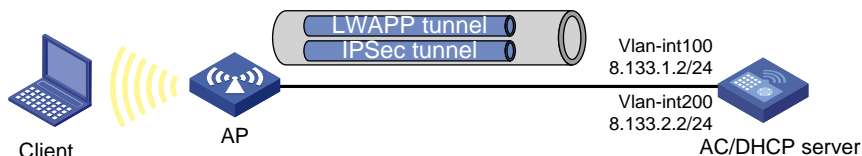
本文档假设您已了解 IPsec 和 WLAN 特性。

## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示组网，Client 和 AP 通过 DHCP 动态获取 IP 地址，要求：配置 IPsec 对 AC 和 AP 间的隧道进行加密保护。

图1 IPsec 加密 AP 与 AC 间隧道组网图



### 3.2 配置思路

- 为了配置 AP 方的 IPsec，需要在 AC 上通过 AP 预配置的方式下发 IPsec 配置到 AP 设备。
- 为了及时检测 IKE 对等体的存活状态，可以配置 IKE DPD 功能。
- 为了使 IPsec 生效，需要将 IPsec 策略应用在 AP 对应的 VLAN 接口下。
- 为了避免 IPsec 隧道一端安全网关出现问题时，造成 IPsec 流量黑洞现象，需要配置 IPsec 无效 SPI 恢复功能。

### 3.3 配置注意事项

- IKE peer 配置的对端地址必须包含 AP 地址；
- AP 和 AC 的配置的预共享密钥需要保持一致；
- AC 上使用命令 **save wlan ap provision** 保存 AP 配置时，需要等待一段时间以保证 AP 能够将下发的配置成功写入存储介质。

- 对于不同的软件版本配置 IPsec 安全提议的命令略有差异，对于较低的软件版本，请使用 **ipsec proposal proposal-name**，对于较高的软件版本，请使用 **ipsec transform-set transform-set-name**，本例使用较高软件版本配置和验证。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### (1) 配置 AC 的基本信息

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan 100
[AC-Vlan-interface100] ip address 8.133.1.2 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN 和 Client 的业务 VLAN，并配置 VLAN 200 接口的 IP 地址。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan 200
[AC-Vlan-interface200] ip address 8.133.2.2 24
[AC-Vlan-interface200] quit
```

# 配置 DHCP 地址池。其中地址池 vlan100 给 AP 分配 8.133.1.0/24 网段地址，地址池 vlan200 给 client 分配 8.133.2.0/24 网段地址。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 8.133.1.0 24
[AC-dhcp-pool-vlan100] quit
[AC] dhcp server ip-pool vlan200
[AC-dhcp-pool-vlan200] network 8.133.2.0 24
[AC-dhcp-pool-vlan200] quit
```

# 启用 DHCP 服务。

```
[AC] dhcp enable
```

### (2) 配置无线服务

# 创建 WLAN-ESS1 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] quit
```

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 配置当前服务模板的 SSID 为 office。

```
[AC-wlan-st-1] ssid office
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

### (3) 配置射频接口并绑定服务模板

# 创建 AP 模板，名称为 testap，型号名称选择 WA2620-AGN，并配置序列号。

```
[AC] wlan ap testap model WA2620E-AGN
```

```
[AC-wlan-ap-testap] serial-id 21023529G007C000020
```

# 进入 radio1 射频视图。

```
[AC-wlan-ap-testap] radio 1
```

# 设置 radio1 接口的信道为 149。

```
[AC-wlan-ap-testap-radio-1] channel 149
```

# 在 radio1 下绑定服务模板 1。

```
[AC-wlan-ap-testap-radio-1] service-template 1
```

# 开启 radio 1。

```
[AC-wlan-ap-testap-radio-1] radio enable
```

```
[AC-wlan-ap-testap-radio-1] quit
```

```
[AC-wlan-ap-testap] quit
```

### (4) 配置 IPsec

# 配置 IKE 心跳报文发送间隔为 20s，超时为 60s。

```
[AC] ike sa keepalive-timer interval 20
```

```
[AC] ike sa keepalive-timer timeout 60
```

# 配置 IPsec 无效 SPI 恢复功能。

```
[AC] ipsec invalid-spi-recovery enable
```

# 配置 IPsec 安全提议的名称为 tran1。

```
[AC] ipsec transform-set tran1
```

# 配置 ESP 协议采用的认证算法为 SHA-1，加密算法为 aes-cbc-128。

```
[AC-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

```
[AC-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
```

```
[AC-ipsec-transform-set-tran1] quit
```

# 创建 IKE 提议，并指定一个供 IKE 提议使用的加密算法为 aes-cbs-128 以及配置 IKE 阶段 1 密钥协商时所使用的 DH 密钥交换参数为 dh group2。

```
[AC] ike proposal 1
```

```
[AC-ike-proposal-1] encryption-algorithm aes-cbc 128
```

```
[AC-ike-proposal-1] dh group2
```

```
[AC-ike-proposal-1] quit
```

# 创建 IKE DPD，并采用其默认配置。

```
[AC] ike dpd dpd
```

```
[AC-ike-dpd-dpd] quit
```

# 创建 IKE 对等体 peer1。

```

[AC] ike peer peer1
# 应用 DPD。
[AC-ike-peer-peer1] dpd dpd
# 应用 proposal。
[AC-ike-peer-peer1] proposal 1
# 配置预共享密钥为 123456。
[AC-ike-peer-peer1] pre-shared-key simple 123456
# 配置对端安全网关 IP 地址为 8.133.1.0~8.133.1.255。
[AC-ike-peer-peer1] remote-address 8.133.1.0 8.133.1.255
[AC-ike-peer-peer1] quit
# 创建 IPsec 策略模板 pt。
[AC] ipsec policy-template pt 1
# 配置 IPsec 安全策略引用名字为 tran1 的 IPsec 安全提议。
[AC-ipsec-policy-template-pt-1] transform-set tran1
# 配置在 IPsec 安全策略中引用名字为 peer1 的 IKE 对等体。
[AC-ipsec-policy-template-pt-1] ike-peer peer1
[AC-ipsec-policy-template-pt-1] quit
# 引用策略模板 pt 创建名字为 map，顺序号为 1 的一条 IPsec 安全策略。
[AC] ipsec policy map 1 isakmp template pt
# 在 VLAN 100 接口上应用名为 map 的 IPsec 策略。
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipsec policy map
[AC-Vlan-interface100] quit
(5) 通过 AP 预配置功能下发 IPsec 的配置
# 进入 AP 预配置视图。
[AC] wlan ap testap
[AC-wlan-ap-testap] provision
# 以明文方式配置 AP 使用 IPsec 加密控制隧道。
[AC-wlan-ap-testap-prvs] tunnel encryption ipsec pre-shared-key simple 123456
# 配置 AP 使用 IPsec 密钥加密数据隧道。
[AC-wlan-ap-testap-prvs] data-tunnel encryption enable
# 将 AP 预配置信息保存到 testap 的私有配置文件中。
[AC-wlan-ap-testap-prvs] save wlan ap provision name testap
[AC-wlan-ap-testap-prvs] return
# 重启 AP 之后，AP 会采用 IPsec 加密上线。
<AC> reset wlan ap name testap
This command will reset all master connection AP's.
Do you want to continue [Y/N]:y

```

## 3.5 验证配置

```

# 使用命令 display ipsec sa brief 可查看存在的 IPsec sa。
[AC] display ipsec sa brief
total phase-2 SAs: 4

```

| Src Address | Dst Address | SPI        | Protocol | Algorithm               |
|-------------|-------------|------------|----------|-------------------------|
| 8.133.1.2   | 8.133.0.2   | 3534306385 | ESP      | E:DES<br>A:HMAC-SHA1-96 |
| 8.133.1.2   | 8.133.0.2   | 2343364398 | ESP      | E:DES<br>A:HMAC-SHA1-96 |
| 8.133.0.2   | 8.133.1.2   | 1289347059 | ESP      | E:DES<br>A:HMAC-SHA1-96 |
| 8.133.0.2   | 8.133.1.2   | 1098232824 | ESP      | E:DES<br>A:HMAC-SHA1-96 |

# 使用命令 **display wlan client** 查看无线客户端可以正常上线。

```
[AC] display wlan client
```

```
Total Number of Clients      : 1
                               Client Information
SSID: office
```

| MAC Address    | User Name | APID/RID | IP Address | VLAN |
|----------------|-----------|----------|------------|------|
| 0022-3f90-938e | -NA-      | 1 /1     | 0.0.0.0    | 200  |

## 3.6 配置文件

```
#
ike sa keepalive-timer interval 20
ike sa keepalive-timer timeout 60
#
ipsec invalid-spi-recovery enable
#
vlan 100
#
vlan 200
#
ike proposal 1
  encryption-algorithm aes-cbc 128
  dh group2
#
ike dpd dpd
#
ike peer peer1
  proposal 1
  pre-shared-key cipher $c$3$MiYotExKrcBnqhWvmo7aZ55fIw0deYmvtg==
  remote-address 8.133.0.0 8.133.255.255
  dpd dpd
#
ipsec transform-set tran1
  encapsulation-mode tunnel
  transform esp
  esp authentication-algorithm sha1
```

```

    esp encryption-algorithm aes-cbc-128
#
ipsec policy-template pt 1
    ike-peer peer1
    transform-set tran1
#
ipsec policy map 1 isakmp template pt
#
dhcp server ip-pool vlan100
    network 8.133.1.0 mask 255.255.255.0
#
dhcp server ip-pool vlan200
    network 8.133.2.0 mask 255.255.255.0
#
wlan service-template 1 clear
    ssid office
    bind WLAN-ESS 1
    service-template enable
#
interface Vlan-interface100
    ip address 8.133.1.2 255.255.255.0
    ipsec policy map
#
interface Vlan-interface200
    ip address 8.133.2.254 255.255.255.0
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
#
wlan ap testap model WA2620E-AGN id 1
    serial-id 21023529G007C000020
    provision
        vlan untagged 1
        tunnel encryption ipsec pre-shared-key cipher xz8n+yXxN+I=
        data-tunnel encryption enable
    radio 1
        channel 149
        service-template 1
        radio enable
    radio 2
#
dhcp enable
#

```



## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# IPv6 源地址验证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 2 |
| 3.3 配置步骤.....          | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 3 |
| 3.4 验证配置 .....         | 4 |
| 3.5 配置文件 .....         | 5 |
| 4 相关资料 .....           | 6 |

# 1 简介

本文档介绍无线控制器 IPv6 源地址验证的典型配置举例。

## 2 配置前提

本文档适用于使用 Comware V5 软件版本的无线控制器和接入点产品，不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IPv6 源地址验证特性。

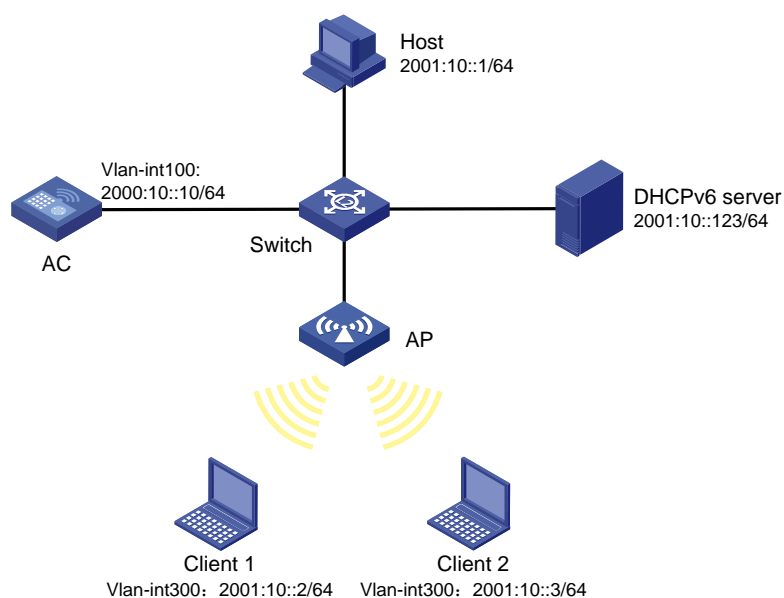
## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC、AP、Host 和 DHCPv6 server 之间均通过交换机连接，Client 1 支持 IPv6 地址的有状态地址配置，DHCPv6 server 给 AP 和 Client 1 动态分配 IPv6 地址，Client 2 手工静态配置 IPv6 地址。要求：

- 客户端通过名称为 service 的 SSID 接入网络。
- 通过 DHCPv6 方式形成绑定表项。
- 开启 IPv6 源地址验证功能，AP 在收到从名称为 service 的 SSID 接入的客户端报文时，转发 Client 1 的报文，丢弃 Client 2 的报文。

图1 IPv6 源地址验证配置组网图



## 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 配置 AC 的 IPv6 功能。

```
<AC> system-view
[AC] ipv6
```

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。AC 将使用该接口的 IPv6 地址与 AP 建立 LWAPP 隧道。

```
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 address 2000:10::10/64
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置 VLAN 300 的接口 IP 地址为 2001:10::1/64。

```
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ipv6 address 2001:10::1/64
```

# 配置 AC 与 Switch 连接的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过，允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

## (2) 配置无线服务

# 创建 **clear** 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 **SSID** 为 **service**。

```
[AC-wlan-st-1] ssid service
```

# 将 **WLAN-ESS1** 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 配置 **IPv6** 源地址验证。

```
[AC-wlan-st-1] ipv6 verify source
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

# 创建 **AP** 的管理模板，名称为 **officeap**，型号名称选择 **WA2620E-AGN**。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 **AP** 的序列号为 **21023529G007C000020**。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 **radio 2** 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 **AC** 上配置的服务模板 1 与射频 2 进行关联。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

# 使能 **AP** 的 **radio 2**。

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

## 3.3.2 Switch 的配置

# 创建 **VLAN 100** 和 **VLAN 300**，其中 **VLAN 100** 用于转发 **AC** 和 **AP** 间 **LWAPP** 隧道内的流量，**VLAN 300** 为无线用户接入的 **VLAN**。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 配置 **Switch** 与 **AC** 相连的 **GigabitEthernet1/0/1** 接口的属性为 **Trunk**，当前 **Trunk** 口的 **PVID** 为 **100**，允许 **VLAN 100** 和 **VLAN 300** 通过。

```
[Switch] interface GigabitEthernet1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 **Switch** 与 **AP** 相连的 **GigabitEthernet1/0/2** 接口属性为 **Access**，并允许 **VLAN 100** 通过。

```
[Switch] interface GigabitEthernet1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 **PoE** 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

### 3.4 验证配置

- (1) Client 1 (0024-d774-e6f4) 上线，并获取到 IPv6 地址 2001:10::2/64;
- (2) Client 2 (0024-0130-696b) 上线，配置静态 IPv6 单播地址 2001:10::3/64;
- (3) 开启 IPv6 源地址验证功能后，在 AC 上查看到客户端的 IPv6 绑定表项信息，表项中 Client 1 的 Type 为 DHCPv6，其上行报文源 IPv6 地址和 MAC 地址与 Client 1 本身的一致，报文可以正常转发；表项中 Client 2 的 Type 为 ND，其上行报文的源 IPv6 地址为 2001:10::/64，与 Client 2 本身的 IPv6 地址 2001:10::3/64 不一致，报文会被丢弃。

```
[AC] display wlan client ipv6 source binding
```

```
Total Number of Clients : 2
```

```
IPv6 Source Binding Information
```

| MAC Address    | APID/RID | Type   | Binding IP Address |
|----------------|----------|--------|--------------------|
| 0024-0130-696b | 1/2      | ND     | 2001:10::/64       |
| 0024-d774-e6f4 | 1/2      | DHCPv6 | 2001:10::2         |

- (4) 从无线客户端 Client 1 上 ping 同网段中的主机 Host，可以 ping 通。

```
C:\Users\>ping -S 2001:10::2 2001:10::1
```

```
Pinging 2001:10::1 from 2001:10::2 with 32 bytes of data:
```

```
Reply from 2001:10::1 : time=22ms
```

```
Reply from 2001:10::1 : time=61ms
```

```
Reply from 2001:10::1 : time=32ms
```

```
Reply from 2001:10::1 : time=16ms
```

```
Ping statistics for 2001:10::1 :
```

```
Packets: Sent = 4,Received = 4,Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 16ms, Maximum = 61ms, Average = 32ms
```

- (5) 从无线客户端 Client 2 上 ping 同网段中的主机 Host，不能 ping 通。

```
C:\Users\>ping -S 2001:10::3 2001:10::1
```

```
Pinging 2001:10::1 from 2001:10::3 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 2001: 10::1 :
```

```
Packets: Sent = 4,Received = 0,Lost = 4 (100% loss),
```

## 3.5 配置文件

- AC:

```
#
ipv6
#
vlan 100
#
vlan 200
#
vlan 300
#
wlan service-template 1 clear
    ssid service
    ipv6 verify source
    bind WLAN-ESS 1
    service-template enable
#
interface Vlan-interface100
    ipv6 address 2000:10::10/64
#
interface Vlan-interface300
    ipv6 address 2001:10::1/64
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200 300
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
    serial-id 21023529G007C000020
    radio 1
    radio 2
        service-template 1 vlan-id 300
    radio enable
```

- Switch:

```
#
vlan 100
#
vlan 300
#
```



```
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。

# IPv6 组播优化典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤 .....         | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 3 |
| 3.4 验证配置 .....         | 4 |
| 3.5 配置文件 .....         | 4 |
| 4 相关资料 .....           | 6 |

# 1 简介

本文档介绍了 IPv6 组播优化典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

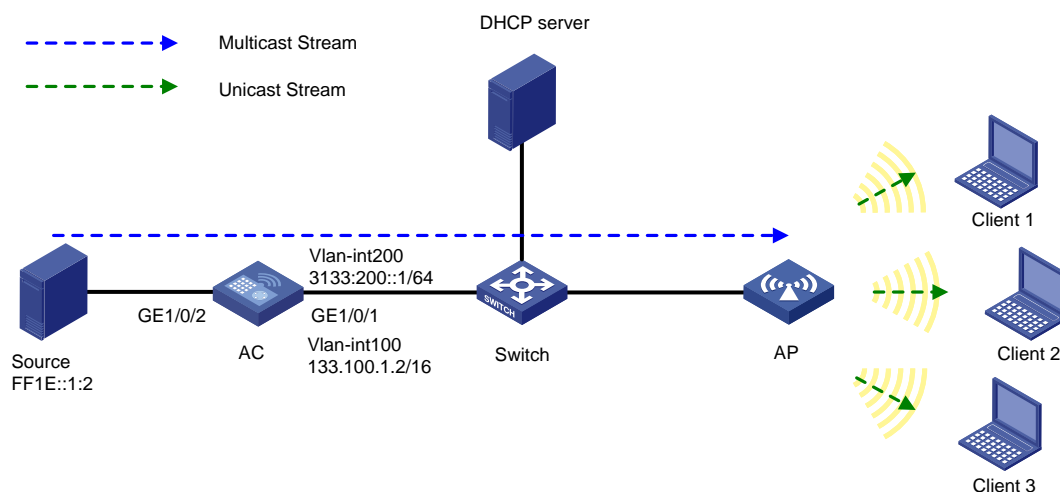
本文档假设您已了解 WLAN 高级功能中的组播优化特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，IPv6 的组播源 Source、AC、Switch 和 AP 工作在同一局域网中，AP 和 Client 通过 DHCP server 获取 IP 地址。为保证组播的报文转播的高效性，要求：开启组播优化功能，在 AP 上将组播数据报文转换为单播数据报文并发送给客户端。

图1 IPv6 组播优化组网图



### 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 133.100.1.2 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN 和 Client 接入的业务 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 配置 VLAN 200 的接口地址分别为 3133:200::1/64。

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ipv6 address 3133:200::1 64
[AC-Vlan-interface200] quit
```

# 配置 AC 与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型为 Trunk 类型，配置 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 和 Client 使用的 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

# 配置 AC 的 GigabitEthernet1/0/2 接口为 Access 类型并加入 VLAN 200。

```
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] port access vlan 200
[AC-GigabitEthernet1/0/2] quit
```

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

#### (2) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

### (3) 配置射频接口并绑定服务模板

# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行绑定。

```
[AC-wlan-ap-officeap-radio-2] service-template 1
```

# 使能 AP 的 radio 2。

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

### (4) 启用组播优化服务以及完成组播相关的配置。

# 在服务模板 1 上开启组播优化功能。

```
[AC] wlan service-template 1
```

```
[AC-wlan-st-1] service-template disable
```

```
[AC-wlan-st-1] multicast optimization enable
```

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

# 全局开启 MLD Snooping。

```
[AC] mld-snooping
```

```
[AC-mld-snooping] quit
```

# 在 VLAN 200 内使能 MLD Snooping，并使能丢弃未知组播数据报文的功能。

```
[AC] vlan 200
```

```
[AC-vlan200] mld-snooping enable
```

```
[AC-vlan200] mld-snooping drop-unknown
```

# 将 MLD Snooping 版本配置为 2，并使能 MLD Snooping 查询器，配置 MLD 普遍组查询报文的源 IP 地址为当前 VLAN 接口的 IP 地址

```
[AC-vlan200] mld-snooping version 2
```

```
[AC-vlan200] mld-snooping querier
```

```
[AC-vlan200] mld-snooping general-query source-ip current-interface
```

```
[AC-vlan200] quit
```

## 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
```

```

[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止
VLAN1 通过，允许 VLAN 100 和 VLAN 200 通过。
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN100
通过。
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit

```

### 3.4 验证配置

# 使用 Client 进行 IPv6 组播点播，使用 **display wlan multicast optimization all** 命令查看 AC 上组播转单播表项生成如下。

```

<AC> display wlan multicast optimization all
                        Multicast Optimization Information
AP Name: officeap
Radio: 2
Total clients: 3
Action: Optimize
Multicast Address: FF1E::1:2
MAC Address:
0021-632f-f7bb, 0023-8933-21ff, 2477-0374-2cc0

```

# 对 Client 上的无线网卡进行抓包，查看目的 IPv6 为组播地址的报文，可以观察到这些报文的目的 MAC 地址为 Client 网卡的 MAC 地址而非组播地址，表示该报文由 AP 进行单播发送。

### 3.5 配置文件

- AC
- #

```

mld-snooping
#
vlan 100
#
vlan 200
    mld-snooping enable
    mld-snooping version 2
    mld-snooping drop-unknown
    mld-snooping querier
    mld-snooping general-query source-ip current-interface
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    multicast optimization enable
    service-template enable
#
interface Vlan-interface100
    ip address 133.100.1.2 255.255.0.0
#
interface Vlan-interface200
    ipv6 address 3133:200::1/64
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk pvid vlan 100
    port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 200
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
    serial-id 21023529G007C000020
    radio 1
    radio 2
        service-template 1
        radio enable
#

```

- Switch



```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# NAT 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项.....        | 2 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 3 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 4 |
| 4 相关资料 .....           | 6 |

# 1 简介

本文介绍了启用 NAT 典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 和 NAT 等特性。

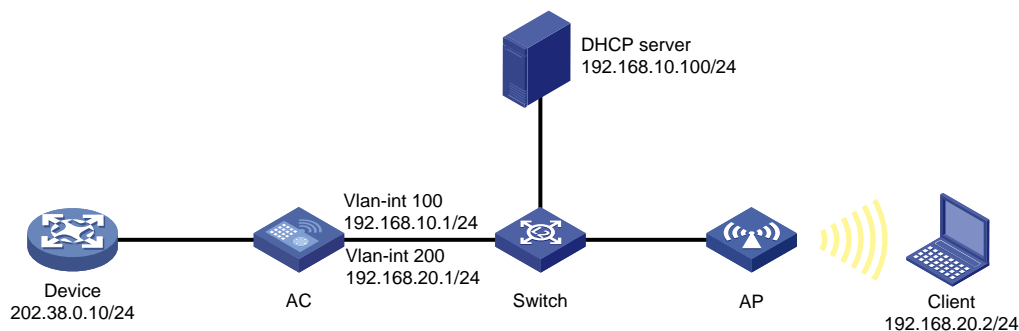
## 3 配置举例

### 3.1 组网需求

如图 1 所示，某公司内部部署无线网络，用户 Client 通过接入无线网络对外网进行访问，AP 和 Client 通过 DHCP 服务器获取 IP 地址。该公司拥有五个公网地址为 202.38.0.1~202.38.0.5。具体要求如下：

- 对访问外网的用户进行限制，只允许 192.168.20.0/24 网段的用户访问外网（本文以一台主机为例）。
- 在 AC 出接口配置 NAT 功能，隐藏内网地址，保护内部网络的安全。

图1 启用 NAT 服务配置组网图



### 3.2 配置思路

由于该公司拥有的公有 IP 地址数目较少，并且为了保证多个内网用户可以同时访问外网，所以需要配置 NAT 地址转换，使多个内部地址映射到同一个公网地址。

### 3.3 配置注意事项

- 要保证目的网络到地址池中地址的路由可达。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.4 配置步骤

#### 3.4.1 AC 的配置

##### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.10.1 255.255.255.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.168.20.1 255.255.255.0
[AC-Vlan-interface200] quit
```

# 创建 VLAN 300 作为 AC 的出接口 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 创建 WLAN-ESS 1 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS 1 接口类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200, 禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

# 配置 AC 连接 Switch 的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置 NAT 功能

# 在 AC 上配置一个从 202.38.0.1 到 202.38.0.5 的地址池，地址池索引号为 1。

```
[AC] nat address-group 1 202.38.0.1 202.38.0.5
```

# 在 AC 上配置 ACL 规则 2001，允许 192.168.20.0/24 网段的主机进行地址转换。

```
[AC] acl number 2001
```

```
[AC-acl-basic-2001] rule permit source 192.168.20.0 0.0.0.255
```

```
[AC-acl-basic-2001] quit
```

# 在 VLAN 接口 300 上配置 ACL 2001 与 IP 地址池 1 相关联。

```
[AC] interface vlan-interface 300
```

```
[AC-Vlan-interface300] nat outbound 2001 address-group 1
```

```
[AC-Vlan-interface300] quit
```

## (3) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

## (4) 配置 AP

# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联。

```
[AC-wlan-ap-officeap-radio-2] service-template 1
```

# 使能 AP 的 radio2。

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

```
[AC-wlan-ap-officeap] quit
```

## 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口链路类型为 Access，当前 Access 口允许 VLAN 100 通过，并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口链路类型为 Access，当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
```

```
[Switch-GigabitEthernet1/0/3] port link-type access
```

```
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

```
[Switch-GigabitEthernet1/0/3] quit
```

### 3.5 验证配置

# Client 成功上线后，Ping 外网设备，并在 AC 上通过命令 **display session table verbose** 查看会话表信息。可以看到转换前 Client 的 IP 地址为 192.168.20.2、端口号为 2048，转换后 IP 地址为 202.38.0.3、端口号为 1025。

```
[AC] display session table verbose
```

```
Initiator:
```

```
Source IP/Port : 192.168.20.2/2048
```

```
Dest IP/Port   : 202.38.0.10/1
```

```
VPN-Instance/VLAN ID/VLL ID:
```

```
Responder:
```

```
Source IP/Port : 202.38.0.10/0
```

```
Dest IP/Port   : 202.38.0.3/1025
```

```
VPN-Instance/VLAN ID/VLL ID:
```

```
Pro: ICMP(1)   App: unknown      State: ICMP-CLOSED
```

```
Start time: 2014-01-24 11:09:40  TTL: 20s
```

```
Received packet(s)(Init): 5 packet(s) 300 byte(s)
```

```
Received packet(s)(Reply): 5 packet(s) 300 byte(s)
```

```
Total find: 1
```

### 3.6 配置文件

- AC:

```
#
```

```

nat address-group 1 202.38.0.1 202.38.0.5 level 1
#
acl number 2001
rule 0 permit source 192.168.20.0 0.255.255.255
#
vlan 100
#
vlan 200
#
vlan 300
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 192.168.10.0 255.255.255.0
#
interface Vlan-interface200
ip address 192.168.20.0 255.255.255.0
#
interface Vlan-interface300
nat outbound 2001 address-group 1
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1
radio enable
#

```

- **Switch:**

```

#
vlan 100
#

```



```
vlan 300
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“ACL 和 QoS 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“ACL 和 QoS 命令参考”。

# MAC 认证+Guest VLAN+本地 Portal 认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                     |    |
|---------------------|----|
| 1 简介.....           | 1  |
| 2 配置前提 .....        | 1  |
| 3 配置举例 .....        | 1  |
| 3.1 组网需求 .....      | 1  |
| 3.2 配置思路 .....      | 1  |
| 3.3 配置注意事项 .....    | 2  |
| 3.4 配置步骤 .....      | 2  |
| 3.4.1 无线接入的配置 ..... | 2  |
| 3.4.2 安全认证的配置 ..... | 4  |
| 3.5 验证配置 .....      | 9  |
| 3.6 配置文件 .....      | 10 |
| 4 相关资料 .....        | 12 |

# 1 简介

本文档介绍当用户 MAC 地址认证失败时进入指定 Guest VLAN，只能访问在 Guest VLAN 的网络资源，只有当用户通过 Portal 认证后才能访问公共网络资源的配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、MAC 地址认证、本地 Portal 认证和 WLAN 特性。

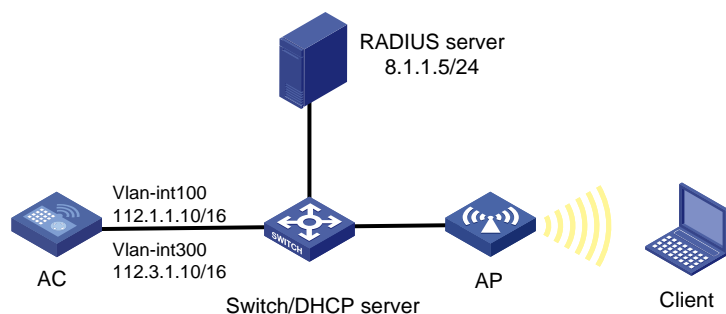
## 3 配置举例

### 3.1 组网需求

如图 1 所示，Client 通过 AP 接入无线网络，设备管理员希望对 Client 进行 MAC 地址认证及 Portal 认证，以控制其对网络资源的访问，具体要求如下：

- 用户 Client 通过 VLAN 200 上线并在 RADIUS server 上进行 MAC 地址认证。
- 用户 Client 的 MAC 地址认证失败时进入 Guest VLAN 300，此时 Client 只能访问 VLAN 300 内的网络资源。
- 用户 Client 在 Guest VLAN 300 中进行 Portal 认证，认证成功后 Client 可以访问公共网络资源。

图1 MAC 认证+Guest VLAN+本地 Portal 认证配置组网图



### 3.2 配置思路

- 为了使 Client 直接 MAC 地址认证失败，需要在 RADIUS server 上配置的用户名和密码是普通的字符串形式，而在 AC 上配置的 MAC 地址认证的用户名和密码是不带连字符的 MAC 地址的形式。

- 为了实现用户在 Guest VLAN 内通过 Portal 认证，需要在 AC 上配置本地 Portal server，在 Guest VLAN 300 上启用 Portal 认证。
- 由于 MAC 地址认证和 Portal 认证的网络服务类型不同，MAC 地址认证为 lan-access 类型，Portal 认证为 portal 类型，所以需要配置两个认证域 office1 和 office2。

### 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.4 配置步骤

#### 3.4.1 无线接入的配置

##### 1. 配置 AC

##### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 112.1.1.10 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并配置其 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 112.3.1.10 16
[AC-Vlan-interface300] quit
```

# 配置 AC 连接 Switch 的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

## (2) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

## (3) 配置射频接口并绑定服务模板

# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN，并配置 AP 的序列号。

```
[AC] wlan ap officeap model WA2620E-AGN
```

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将服务模板 1 绑定到 AP 的 Radio 2 口，并使能 Radio 2。

```
[AC-wlan-ap-officeap-radio-2] service-template 1
```

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

## 2. 配置 Switch

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface GigabitEthernet1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 使能 DHCP 服务。

```
[Switch] dhcp enable
```

# 创建名为 **vlan100** 的 DHCP 地址池，配置地址池范围为 **112.1.1.1~112.1.1.9**，网关地址为 **112.1.1.10**，为 AP 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan100 extended
```

```
[Switch-dhcp-pool-vlan100] network ip range 112.1.1.1 112.1.1.9
```

```
[Switch-dhcp-pool-vlan100] network mask 255.255.0.0
```

```
[Switch-dhcp-pool-vlan100] gateway-list 112.1.1.10
```

```
[Switch-dhcp-pool-vlan100] quit
```

# 创建名为 **vlan300** 的 DHCP 地址池，配置地址池范围为 **112.3.1.1~112.3.1.9**，网关地址为 **112.3.1.10**，为 Client 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan300 extended
```

```
[Switch-dhcp-pool-vlan300] network ip range 112.3.1.1 112.3.1.9
```

```
[Switch-dhcp-pool-vlan300] network mask 255.255.0.0
```

```
[Switch-dhcp-pool-vlan300] gateway-list 112.3.1.10
```

```
[Switch-dhcp-pool-vlan300] quit
```

### 3.4.2 安全认证的配置

#### 1. 配置 AC

##### (1) 配置认证策略和认证域

# 在 AC 上创建 RADIUS 方案 **office** 并进入其视图。

```
<AC> system-view
```

```
[AC] radius scheme office
```

# 配置主认证、计费 RADIUS 服务器的 IP 地址为 **8.1.1.5**。

```
[AC-radius-office] primary authentication 8.1.1.5
```

```
[AC-radius-office] primary accounting 8.1.1.5
```

# 配置 RADIUS 认证、计费报文的共享密钥为 **123456789**。

```
[AC-radius-office] key authentication simple 123456789
```

```
[AC-radius-office] key accounting simple 123456789
```

# 配置发送给 RADIUS 服务器的用户名不得携带域名。

```
[AC-radius-office] user-name-format without-domain
```

# 设置设备发送 RADIUS 报文使用的源 IP 地址。

```
[AC-radius-office] nas-ip 112.1.1.10
```

```
[AC-radius-office] quit
```

# 创建 **office1** 域并进入其视图。

```
[AC] domain office1
```

# 在 ISP 域 **office1** 下，为 **lan-access** 用户配置认证、授权、计费方案为 RADIUS 方案，方案名为 **office**。

```
[AC-isp-office1] authentication lan-access radius-scheme office
```

```
[AC-isp-office1] authorization lan-access radius-scheme office
```

```
[AC-isp-office1] accounting lan-access radius-scheme office
```

# 设置当前 ISP 域下的用户闲置切断功能，闲置检测时间为 **60** 分钟。

```
[AC-isp-office1] idle-cut enable 60
```

```
[AC-isp-office1] quit
# 创建 office2 域并进入其视图。
[AC] domain office2
# 在 ISP 域 office2 下, 为 Portal 用户配置认证、授权、计费方案为 RADIUS 方案, 方案名为 office。
[AC-isp-office2] authentication portal radius-scheme office
[AC-isp-office2] authorization portal radius-scheme office
[AC-isp-office2] accounting portal radius-scheme office
# 设置当前 ISP 域下的用户闲置切断功能, 闲置检测时间为 60 分钟。
[AC-isp-office2] idle-cut enable 60
[AC-isp-office2] quit
(2) 配置 MAC 地址认证
# 全局使能端口安全功能。
[AC] port-security enable
# 配置 MAC 地址认证用户名格式, 使用不带连字符的 MAC 地址作为用户名与密码。
[AC] mac-authentication user-name-format mac-address without-hyphen
# 进入 WLAN-ESS1 接口。
[AC] interface wlan-ess 1
# 配置端口安全模式为 MAC 地址认证, 并指定 MAC 地址认证用户使用的认证域为 office1。
[AC-WLAN-ESS1] port-security port-mode mac-authentication
[AC-WLAN-ESS1] mac-authentication domain office1
# 配置 MAC 地址认证失败后, 用户进入 Guest VLAN 300。
[AC-WLAN-ESS1] mac-authentication guest-vlan 300
[AC-WLAN-ESS1] quit
(3) 配置本地 Portal 认证
# 配置本地 Portal server。
[AC] portal server portal ip 112.3.1.10
# 配置本地 Portal 服务器支持 HTTP 协议类型。
[AC] portal local-server http
# 配置 Guest VLAN 所在的接口 VLAN 300 上启用 Portal 认证, 并配置为直接认证方式。
[AC] interface vlan-interface 300
[AC-Vlan-interface300] portal server portal method direct
# 配置从接口 VLAN 300 接入的 IPv4 Portal 用户使用认证域为 office2。
[AC-Vlan-interface300] portal domain office2
[AC-Vlan-interface300] quit
# 配置 Portal 免认证规则, 使得符合源接口为 GigabitEthernet1/0/1 (GigabitEthernet1/0/1 接口为 AC 与交换机互通的接口) 的报文不会触发 Portal 认证。
[AC] portal free-rule 0 source interface GigabitEthernet1/0/1
```

## 2. 在 RADIUS server 上配置设备接入和用户管理



说明

下面以 iMC 为例(使用 iMC 版本为: iMC PLAT 5.2(E0401)、iMC UAM 5.2(E0402), 说明 RADIUS server 的基本配置。



# 增加接入设备。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[用户接入管理/接入设备管理/接入设备配置]菜单项，单击<增加>按钮，进入“增加接入设备”页面，单击<手工增加>按钮，进入“手工增加接入设备”页面。

- 填写起始 IP 地址为 112.1.1.10，该 IP 地址为 AC 上配置的 radius scheme 视图下的 nas-ip 地址。
- 单击<确定>按钮完成操作。
- 在“接入配置”页面配置共享密钥为 123456789，该共享密钥与 AC 上配置 Radius 服务器时的密钥一致。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

业务 >> 用户接入管理 >> 接入设备管理 >> 接入设备配置 >> 增加接入设备

接入配置

认证端口

1812

共享密钥

●●●●●●●●

接入区域

无

接入设备类型

H3C(General)

业务分组

未分组

计费端口

1813

确认共享密钥

●●●●●●●●

业务类型

LAN接入业务

组网方式

不启用混合组网

设备列表

选择

手工增加

全部清除

共有1条记录。

| 设备名称 | 设备IP地址     | 设备型号 | 备注 | 删除 |
|------|------------|------|----|----|
|      | 112.1.1.10 |      |    | ✖  |

确定

取消

# 增加接入规则配置。

选择“业务”页签，单击导航树中的[用户接入管理/接入规则管理]菜单项，单击<增加>按钮，创建一条接入规则。

- 接入规则名输入“office”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

业务 >> 用户接入管理 >> 接入规则管理 >> 增加接入规则

|                                         |                                                                                                   |                                  |   |
|-----------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------|---|
| <b>基本信息</b>                             |                                                                                                   |                                  |   |
| * 接入规则名                                 | office                                                                                            |                                  |   |
| * 业务分组                                  | 未分组                                                                                               |                                  |   |
| 描述                                      |                                                                                                   |                                  |   |
| <b>授权信息</b>                             |                                                                                                   |                                  |   |
| 接入时段                                    | 无                                                                                                 | * 分配IP地址                         | 否 |
| 下行速率                                    |                                                                                                   | 上行速率                             |   |
| 优先级                                     |                                                                                                   | <input type="checkbox"/> 启用RSA认证 |   |
| 证书认证                                    | <input checked="" type="radio"/> 不启用 <input type="radio"/> EAP证书认证 <input type="radio"/> WAPI证书认证 |                                  |   |
| 认证证书类型                                  | EAP-TLS认证                                                                                         |                                  |   |
| 下发VLAN                                  |                                                                                                   |                                  |   |
| <input type="checkbox"/> 下发User Profile |                                                                                                   | 下发用户组                            |   |
| <input type="checkbox"/> 下发ACL          |                                                                                                   |                                  |   |

# 增加服务配置。

选择“业务”页签，单击导航树中的[用户接入管理/服务配置管理]菜单项，单击<增加>按钮，创建一条服务。

- 配置服务名为 09797\_portal（任意命名）。
- 缺省接入规则选择“office”。
- 其他采用默认配置。
- 单击<确定>按钮完成配置。

业务 >> 用户接入管理 >> 服务配置管理 >> 增加服务配置

|                                         |                                         |          |        |
|-----------------------------------------|-----------------------------------------|----------|--------|
| <b>基本信息</b>                             |                                         |          |        |
| * 服务名                                   | 09797_portal                            | 服务后缀     |        |
| * 业务分组                                  | 未分组                                     | * 缺省接入规则 | office |
| * 缺省私有属性下发策略                            | 不使用                                     |          |        |
| 计费策略                                    | 不计费                                     |          |        |
| 服务描述                                    |                                         |          |        |
| <input checked="" type="checkbox"/> 可申请 | <input type="checkbox"/> Portal智能终端快速认证 |          |        |
| <b>接入策略列表</b>                           |                                         |          |        |
| 增加                                      |                                         |          |        |
| 接入场景                                    | 接入规则                                    | 私有属性下发策略 | 优先级    |
| 修改                                      | 删除                                      |          |        |
| 确定                                      |                                         | 取消       |        |

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户]菜单项，单击“接入用户列表”下面的<增加>按钮，增加一个接入用户。

- 单击<选择>按钮。
- 输入用户姓名 shl，单击<查询>按钮。
- 页面返回查询结果，如果用户存在，则选中用户，单击<确定>按钮。

用户 >> 所有接入用户 >> 增加接入用户

接入用户

接入信息

\* 用户姓名  选择 增加用户

选择用户 - Windows Internet Explorer

http://8.1.1.5:8080/imc/usr/user/addUserPopUpContent.jsf

选择用户 高级查询

用户姓名  证件号码  查询 清除结果

用户列表

共有1条记录，当前第1 - 1，第 1/1 页。 每页显示: 8 15 [50] 100 200

|                                  | 用户姓名 | 证件号码   | 通讯地址 | 用户分组 |
|----------------------------------|------|--------|------|------|
| <input checked="" type="radio"/> | shl  | 111111 |      | 未分组  |

确定 取消

- 如果用户不存在，需单击<增加用户>按钮创建一个。
- 输入用户姓名和证件号码，单击<确定>完成。

用户 >> 所有接入用户 >> 增加接入用户

接入用户

接入信息

\* 用户姓名  选择 增加用户

增加用户 - Windows Internet Explorer

http://8.1.1.5:8080/imc/usr/user/addUserPopUpContent.jsf

增加用户

基本信息

\* 用户姓名  \* 证件号码

通讯地址  电话

电子邮件  \* 用户分组

确定 取消

- 配置帐号名和密码，本例中帐号名和密码都为 shlportal。

- 勾选绑定服务名 09797\_portal。
- 单击<确定>按钮完成。

用户 >> 所有接入用户 >> 增加接入用户

### 接入用户

#### 接入信息

\* 用户姓名: shi [选择] [增加用户]

\* 帐号名: shiportal

☐ 预开用户 ☐ 缺省BYOD用户 ☐ 主机名用户 ☐ 快速认证用户

\* 密码: ..... \* 密码确认: .....

☒ 允许用户修改密码 ☐ 启用用户密码控制策略 ☐ 下次登录须修改密码

失效日期: [ ] [?] Portal智能终端最大绑定数: 1 [?]

最大闲置时长: [ ] 分钟 在线数量限制: 1

帐号类型: 预付费 \* 预付金额: 0 元

自助充值: 允许

登录提示信息: [ ]

#### 接入服务

|                                     | 服务名          | 服务后缀 | 状态  | 计费策略 | 分配IP地址 |
|-------------------------------------|--------------|------|-----|------|--------|
| <input checked="" type="checkbox"/> | 09797_portal |      | 可申请 | 不计费  |        |

## 3.5 验证配置

# 完成以上配置后，无线用户 Client 上线进行 MAC 地址认证，由于 RADIUS server 上配置的用户名和密码是普通的字符串形式，而在 AC 上配置的 MAC 地址认证的用户名和密码是不带连字符的 MAC 地址的形式，因此认证失败，无线用户 Client 进入 Guest VLAN300。

在 AC 上通过命令 **display wlan client** 可以看见无线用户 Client 从 Guest VLAN 300 上线。

[AC]

```
%Nov 25 17:28:07:190 2013 AC WMAC/6/WMAC_CLIENT_JOIN_WLAN: Client 3ca9-f414-4c20
successfully joins WLAN service, on APID 1 with BSSID 8434-9700-c550.
```

[AC] display wlan client

```
Total Number of Clients          : 1
```

```
Client Information
```

```
SSID: service
```

```
-----
MAC Address      User Name          APID/RID IP Address          VLAN
-----
3ca9-f414-4c20  3ca9f4144c20        1    /2    112.3.0.2          300
-----
```

# 在 Guest VLAN 300 中的无线用户 Client 在通过 Portal 认证之前只能访问 VLAN 300 的网络资源。

# 在 Guest VLAN 300 中的无线用户 Client 通过 Portal 认证后，可以通过命令 **display portal user all** 查看 Portal 认证信息。

```
%Nov 26 09:28:06:858 2013 AC PORTAL/5/PORTAL_USER_LOGON_SUCCESS:
-UserName=admin-IPAddr=112.3.0.2-IfName=Vlan-interface300-VlanID=300-MACAddr=3ca9-f414-4
c20-APMAC=B4B5-2F4F-2D8C-SSID=service-NasId=-NasPortId=; User got online successfully.
```

[AC] display portal user all

```
Index:1165
```

```
State:ONLINE
```

```
SubState:NONE
```

```

ACL:NONE
Work-mode:stand-alone
MAC                IP                Vlan    Interface
-----
3ca9-f414-4c20    112.3.0.2        300     Vlan-interface300
Total 1 user(s) matched, 1 listed.

```

## 3.6 配置文件

- AC:

```

#
portal server portal ip 112.3.1.10
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
portal local-server http
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
primary authentication 8.1.1.5
primary accounting 8.1.1.5
key authentication cipher $c$3$Zwf/JlgLh0obRwOY8qBSTzrYKvNqWQZHHpdNhQ==
key accounting cipher $c$3$GfKl0XsDx+9P85+f5cAMXlzb4thEC/XrK9LUA==
user-name-format without-domain
nas-ip 112.1.1.10
#
domain office1
authentication lan-access radius-scheme office
authorization lan-access radius-scheme office
accounting lan-access radius-scheme office
access-limit disable
state active
idle-cut enable 60 10240
self-service-url disable
domain office2
authentication portal radius-scheme office
authorization portal radius-scheme office
accounting portal radius-scheme office
access-limit disable
state active
idle-cut enable 60 10240
self-service-url disable
#
wlan service-template 1 clear
ssid service

```

```

bind WLAN-ESS 1
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200 300
#
interface Vlan-interface100
ip address 112.1.1.10 255.255.0.0
#
interface Vlan-interface300
ip address 112.3.1.10 255.255.0.0
portal server portal method direct
portal domain office2
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
port-security port-mode mac-authentication
mac-authentication guest-vlan 300
mac-authentication domain office1
#
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1
radio enable
#

```

- **Switch:**

```

#
vlan 100
#
vlan 300
#
dhcp server ip-pool vlan100 extended
network ip range 112.1.1.1 112.1.1.9
network mask 255.255.0.0
gateway-list 112.1.1.10
#
dhcp server ip-pool vlan300 extended
network ip range 112.3.1.1 112.3.1.9
network mask 255.255.0.0
gateway-list 112.3.1.10
#

```

```
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 100 300
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
  poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。

# Portal 服务器对从不同 AP 和不同认证域上线的用户进行 Portal 认证的典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

|                        |    |
|------------------------|----|
| 1 简介.....              | 1  |
| 2 配置前提 .....           | 1  |
| 3 配置举例 .....           | 1  |
| 3.1 组网需求 .....         | 1  |
| 3.2 配置思路 .....         | 2  |
| 3.3 配置注意事项.....        | 2  |
| 3.4 配置步骤 .....         | 2  |
| 3.4.1 AC 的配置 .....     | 2  |
| 3.4.2 Switch 的配置 ..... | 6  |
| 3.4.3 iMC 的配置 .....    | 6  |
| 3.5 验证配置 .....         | 10 |
| 3.6 配置文件 .....         | 11 |
| 4 相关资料 .....           | 14 |

# 1 简介

本文档介绍不同热点的用户使用同一个 SSID 接入无线网络,并通过不同的 Portal 服务器进行 Portal 接入认证的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应,如果使用过程中与产品实际情况有差异,请参考相关产品手册,或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证,配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置,为了保证配置效果,请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、Portal 和 WLAN 特性。

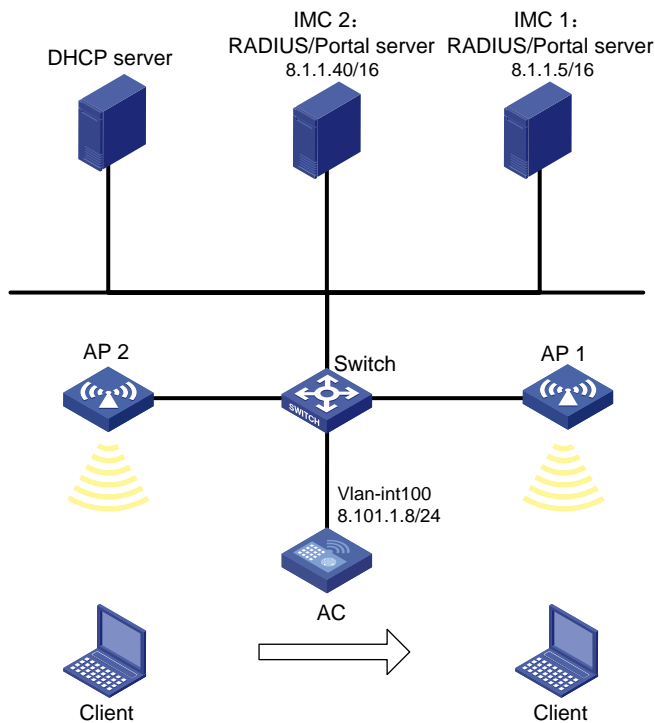
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示,Client 通过热点 AP 1 和 AP 2 使用名称为 service 的 SSID 接入网络,Client 和 AP 通过 DHCP 服务器获取 IP 地址。要求:

- 当 Client 从 AP 2 上线时,由服务器 IMC 2 进行 Portal 认证。
- 当 Client 从 AP 1 上线时,由服务器 IMC 1 进行 Portal 认证。

图1 基于 AP 绑定 Portal 服务器和认证服务器组网图



## 3.2 配置思路

- 由于 Client 从不同的 AP 上线时使用同一个 SSID 接入无线网络，为了进行 Portal 认证时对不同的 AP 加以区分，可以配置 AC 向 RADIUS 服务器发送的 RADIUS 请求报文的 NAS-Identifier 属性值。
- 为了使 Client 从不同的 AP 上线时访问不同的 Portal 服务器，需要配置不同的 Portal 服务器和认证域。
- 由于无线客户端在跨 VLAN 漫游过程中需要通过 MAC VLAN 表项强制保持自身的 VLAN 不变，所以需要在 AC 上开启 MAC-VLAN 功能。

## 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
```

```
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 8.101.1.8 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口为 trunk 模式, 允许 VLAN 100、VLAN 200、VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置无线接口

# 创建 WLAN-ESS1 接口

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200, 禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

## (3) 配置无线服务模板

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 配置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

## (4) 配置射频接口并绑定服务模板

# 创建 AP 1 的管理模板, 名称为 officeap1, 型号名称选择 WA2620E-AGN, 并配置 AP 1 的序列号。

```
[AC] wlan ap officeap1 model WA2620E-AGN
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap1] radio 2
```

# 绑定服务模板 **service-template 1**，指定 VLAN-ID 为 300，指定 NAS-ID 为 **office1**。

```
[AC-wlan-ap-officeap1-radio-2] service-template 1 vlan-id 300 nas-id office1
```

# 使能 AP 1 的 radio 2。

```
[AC-wlan-ap-officeap1-radio-2] radio enable
```

```
[AC-wlan-ap-officeap1-radio-2] quit
```

```
[AC-wlan-ap-officeap1] quit
```

# 创建 AP 2 的管理模板，名称为 **officeap2**，型号名称选择 **WA2620E-AGN**，并配置 AP 2 的序列号。

```
[AC] wlan ap officeap2 model WA2620E-AGN
```

```
[AC-wlan-ap-officeap2] serial-id 21023529G007C000021
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap2] radio 2
```

# 绑定服务模板 **service-template 1**，指定 VLAN-ID 为 300，指定 NAS-ID 为 **office2**。

```
[AC-wlan-ap-officeap2-radio-2] service-template 1 vlan-id 300 nas-id office2
```

# 使能 AP 2 的 radio 2。

```
[AC-wlan-ap-officeap2-radio-2] radio enable
```

```
[AC-wlan-ap-officeap2-radio-2] quit
```

```
[AC-wlan-ap-officeap2] quit
```

## (5) 配置 RADIUS 认证方案及 ISP 域

# 创建名为 **office1** 的 RADIUS 方案并进入该视图。

```
[AC] radius scheme office1
```

# 配置 RADIUS 的服务类型为 **extended**。

```
[AC-radius-office1] server-type extended
```

# 配置 RADIUS 方案的主认证服务器为 **8.1.1.5** 及通信密钥。

```
[AC-radius-office1] primary authentication 8.1.1.5
```

```
[AC-radius-office1] key authentication simple 1234567
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC-radius-office1] user-name-format without-domain
```

# 配置 **nas-ip** 为 VLAN 100 的地址。

```
[AC-radius-office] nas-ip 8.101.1.8
```

```
[AC-radius-office1] quit
```

# 创建 **office1** 域并进入其视图。

```
[AC] domain office1
```

# 为 Portal 用户配置认证方案为 RADIUS 方案，方案名为 **office1**。

```
[AC-isp-office1] authentication portal radius-scheme office1
```

# 为 Portal 用户配置授权方案为 RADIUS 方案，方案名为 **office1**。

```
[AC-isp-office1] authorization portal radius-scheme office1
```

# 为 Portal 用户配置计费为 **none**，不计费。

```
[AC-isp-office1] accounting portal none
```

```
[AC-isp-office1] quit
```

# 创建名为 **office2** 的 RADIUS 方案并进入该视图。

```
[AC] radius scheme office2
```

```

# 配置 RADIUS 的服务类型为 extended。
[AC-radius-office2] server-type extended
# 配置 RADIUS 方案的主认证服务器为 8.1.1.40 及通信密钥。
[AC-radius-office2] primary authentication 8.1.1.40
[AC-radius-office2] key authentication simple 1234567
# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。
[AC-radius-office2] user-name-format without-domain
# 配置 nas-ip 为 VLAN 100 的地址。
[AC-radius-office] nas-ip 8.101.1.8
[AC-radius-office1] quit
# 创建 office2 域并进入其视图。
[AC] domain office2
# 为 Portal 用户配置认证方案为 RADIUS 方案，方案名为 office2。
[AC-isp-office2] authentication portal radius-scheme office2
# 为 Portal 用户配置授权方案为 RADIUS 方案，方案名为 office2。
[AC-isp-office2] authorization portal radius-scheme office2
# 为 Portal 用户配置计费为 none，不计费。
[AC-isp-office2] accounting portal none
[AC-isp-office2] quit
(6) 配置 Portal 认证服务
# 配置名称为 office1 的 Portal 服务器地址为 8.1.1.5、密钥为 1234567 及 url 为
http://8.1.1.5:8080/portal。
[AC] portal server office1 ip 8.1.1.5 key simple 1234567 url http://8.1.1.5:8080/portal
# 配置名称为 office2 的 Portal 服务器地址为 8.1.1.40、密钥为 1234567 及 url 为
http://8.1.1.40:8080/portal。
[AC] portal server office2 ip 8.1.1.40 key simple 1234567 url http://8.1.1.40:8080/portal
# 在 VLAN 300 的接口上使能直接 Portal 认证。
[AC] interface vlan-interface 300
[AC-Vlan-interface300] portal server office2 method direct
# 配置 Portal 用户使用的认证域为 office2。
[AC-Vlan-interface300] portal domain office2
# 配置接口发送 Portal 报文使用的 IPv4 源地址为 8.101.1.8。
[AC-Vlan-interface300] portal nas-ip 8.101.1.8
[AC-Vlan-interface300] quit
# 配置免认证规则，允许 GigabitEthernet1/0/1 口出方向及发往 IMC 1 的报文免认证通过。
[AC] portal free-rule 1 source interface GigabitEthernet1/0/1
[AC] portal free-rule 2 source ip any destination ip 8.1.1.5 mask 255.255.255.255
# 配置全局下 Portal 指定接入 SSID 为 service，当 NAS-ID 为 office1 时使用 Portal server 为 office1，
认证 domain 为 office1。
[AC] portal wlan ssid service spot office1 server office1 domain office1
# 配置全局下 Portal 指定接入 SSID 为 service，当 NAS-ID 为 office2 时使用 Portal server 为 office2，
认证 domain 为 office2。
[AC] portal wlan ssid service spot office2 server office2 domain office2

```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 作为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 的 GigabitEthernet1/0/1 接口的属性为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Access, 并允许 VLAN100 通过。

```
[Switch] interface GigabitEthernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

### 3.4.3 iMC 的配置



下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.2(E0401)、iMC UAM 5.2(E0402)），说明 RADIUS 服务器的基本配置。

---

#### (1) 增加接入设备

登录进入 iMC 管理平台, 选择“业务”页签, 单击导航树中的[用户接入管理/接入设备管理/接入设备配置/接入设备列表]菜单项, 单击<增加>按钮, 进入“增加接入设备”页面, 单击<手工增加>按钮, 进入“手工增加接入设备”页面。

- 填写起始 IP 地址为 8.101.1.8, 该 IP 地址为 AC 上配置的 radius scheme 视图下的 nas-ip 地址。

- 单击<确定>按钮完成操作。
- 在“接入配置”页面配置共享密钥为 1234567，该共享密钥与 AC 上配置 RADIUS 服务器时的密钥一致。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

业务 >> 用户接入管理 >> 接入设备管理 >> 接入设备配置 >> 增加接入设备

| 接入配置   |              |          |         |
|--------|--------------|----------|---------|
| * 认证端口 | 1812         | * 计费端口   | 1813    |
| * 共享密钥 | *****        | * 确认共享密钥 | *****   |
| 接入区域   | 无            | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 组网方式     | 不启用混合组网 |
| 业务分组   | 未分组          |          |         |

| 设备列表    |           |      |    |    |
|---------|-----------|------|----|----|
| 选择      | 手工增加      | 全部清除 |    |    |
| 共有1条记录。 |           |      |    |    |
| 设备名称    | 设备IP地址    | 设备型号 | 备注 | 删除 |
|         | 8.101.1.8 |      |    |    |

## (2) 配置“接入规则管理”

- 选择“业务”页签，单击导航树中的[用户接入管理/接入规则管理]菜单项，单击<增加>按钮，创建一条接入规则。
- 配置接入规则名为 lyportal（任意命名）。
- 其他采用默认配置。
- 单击<确定>按钮完成。

| 基本信息    |          |
|---------|----------|
| * 接入规则名 | lyportal |
| * 业务分组  | 未分组      |
| 描述      |          |

| 授权信息                                    |                                                                                                   |
|-----------------------------------------|---------------------------------------------------------------------------------------------------|
| 接入时段                                    | 无                                                                                                 |
| 下行速率                                    | Kbps                                                                                              |
| 优先级                                     |                                                                                                   |
| 证书认证                                    | <input checked="" type="radio"/> 不启用 <input type="radio"/> EAP证书认证 <input type="radio"/> WAPI证书认证 |
| 认证证书类型                                  | EAP-TLS认证                                                                                         |
| 下发VLAN                                  |                                                                                                   |
| <input type="checkbox"/> 下发User Profile |                                                                                                   |
| <input type="checkbox"/> 下发ACL          |                                                                                                   |
| * 分配IP地址                                | 否                                                                                                 |
| 上行速率                                    | Kbps                                                                                              |
| <input type="checkbox"/> 启用RSA认证        |                                                                                                   |
| 下发用户组                                   |                                                                                                   |

## (3) 增加服务配置

选择“业务”页签，单击导航树中的[用户接入管理/服务配置管理]菜单项，单击<增加>按钮，创建一条服务。

- 配置服务名为 lyportal（任意命名）。
- 缺省接入规则选择步骤(2)中配置的规则名。
- 其他采用默认配置



- 单击<确定>按钮完成配置。

**基本信息**

|                                         |                                         |          |          |
|-----------------------------------------|-----------------------------------------|----------|----------|
| * 服务名                                   | lyportal                                | 服务后缀     |          |
| * 业务分组                                  | 未分组                                     | * 缺省接入规则 | lyportal |
| * 缺省私有属性下发策略                            | 不使用                                     |          |          |
| 服务描述                                    |                                         |          |          |
| <input checked="" type="checkbox"/> 可申请 | <input type="checkbox"/> Portal智能终端快速认证 |          |          |

**接入策略列表**

| 增加                                       |      |          |     |    |    |
|------------------------------------------|------|----------|-----|----|----|
| 接入场景                                     | 接入规则 | 私有属性下发策略 | 优先级 | 修改 | 删除 |
| <div> <div>确定</div> <div>取消</div> </div> |      |          |     |    |    |

#### (4) 增加接入用户

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户/接入用户列表]菜单项，单击<增加>按钮，增加一个接入用户。

- 选择一个用户名 ly。如没有用户名，需单击<增加用户>按钮创建一个。
- 配置帐号名和密码。
- 勾选绑定步骤(3)中创建的服务名。
- 单击<确定>按钮完成。

用户 >> 所有接入用户 >> 增加接入用户

**接入用户**

**接入信息**

|                                              |                                     |                                    |                                 |
|----------------------------------------------|-------------------------------------|------------------------------------|---------------------------------|
| * 用户名                                        | ly                                  | 选择                                 | 增加用户                            |
| * 帐号名                                        | lyportal                            |                                    |                                 |
| <input type="checkbox"/> 预开用户                | <input type="checkbox"/> 缺省BYOD用户   | <input type="checkbox"/> 主机名用户     | <input type="checkbox"/> 快速认证用户 |
| * 密码                                         | *****                               | * 密码确认                             | *****                           |
| <input checked="" type="checkbox"/> 允许用户修改密码 | <input type="checkbox"/> 启用用户密码控制策略 | <input type="checkbox"/> 下次登录须修改密码 |                                 |
| 失效日期                                         |                                     | Portal智能终端最大绑定数                    | 1                               |
| 最大闲置时长                                       | 分钟                                  | 在线数量限制                             | 1                               |
| 登录提示信息                                       |                                     |                                    |                                 |

**接入服务**

| 服务名                                          | 服务后缀 | 状态  | 分配IP地址 |
|----------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> lyportal |      | 可申请 |        |

**接入设备绑定信息**

|           |  |     |  |
|-----------|--|-----|--|
| 设备序列号     |  | 端口号 |  |
| 外层VLAN ID |  |     |  |

#### (5) 配置 Portal 认证的地址组范围

选择“业务”页签，单击导航树中的[用户接入管理/Portal 服务管理/IP 地址组配置]菜单项，单击<增加>按钮，配置进行 Portal 认证的地址组范围。

- 配置 IP 地址组名为 ipgroup。
- 配置起始地址为 101.2.0.0，终止地址为 101.2.255.255。
- 其他采用默认配置。
- 单击<确定>按钮完成。

### 增加IP地址组

|          |               |
|----------|---------------|
| * IP地址组名 | ipgroup       |
| * IPv6   | 否             |
| * 起始地址   | 101.2.0.0     |
| * 终止地址   | 101.2.255.255 |
| 业务分组     | 未分组           |
| * 类型     | 普通            |

确定

取消

### (6) 配置接入设备信息

选择“业务”页签，单击导航树中的[用户接入管理/Portal 服务管理/设备配置]菜单项，单击<增加>按钮，配置 Portal 认证的接入设备。

- 配置设备名为 AC。
- 配置 IP 地址为 8.101.1.8，该地址与 AC VLAN 100 虚接口下配置的 Portal nas-ip 一致。
- 配置密钥为 1234567，该密钥与 AC 上配置 Portal 服务器时设置的密钥一致。
- 其他采用默认配置即可。
- 单击<确定>按钮完成。

### 增加设备信息


#### 设备信息

|          |            |               |           |
|----------|------------|---------------|-----------|
| * 设备名    | AC         | * 业务分组        | 未分组       |
| * 版本     | Portal 2.0 | * IP地址        | 8.101.1.8 |
| * 监听端口   | 2000       | * 本地Challenge | 否         |
| * 认证重发次数 | 0          | * 下线重发次数      | 1         |
| * 支持逃生心跳 | 否          | * 支持用户心跳      | 否         |
| * 密钥     | *****      | * 确认密钥        | *****     |
| * 组网方式   | 三层         |               |           |
| 设备描述     |            |               |           |

确定

取消

### (7) 配置端口组

返回[用户接入管理/Portal 服务管理/设备配置]菜单项，进入“设备信息列表”，选中设备所在的行，单击“操作”图标，选中“ 端口组信息管理”按钮，进入“端口组信息配置”页签。

在“端口组信息列表”子页签，单击<增加>按钮，进入到“增加端口组信息”页面。

- 配置端口组名为 portgroup。
- 配置 IP 地址组，选取步骤(5)中创建的地址组 ipgroup。

- 其他采用默认配置即可。
- 单击<确定>按钮完成。

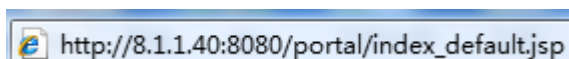
业务 >> 用户接入管理 >> Portal服务管理 >> 设备配置 >> 端口组信息配置 >> 增加端口组信息

| 增加端口组信息  |                   |          |         |
|----------|-------------------|----------|---------|
| * 端口组名   | portgroup         | * 提示语言   | 动态检测    |
| * 开始端口   | 0                 | * 终止端口   | zzzzz   |
| * 协议类型   | HTTP              | * 快速认证   | 否       |
| * 是否NAT  | 否                 | * 错误透传   | 是       |
| * 认证方式   | CHAP认证            | * IP地址组  | ipgroup |
| * 心跳间隔   | 10 分钟             | * 心跳超时   | 30 分钟   |
| 用户域名     |                   | 端口组描述    |         |
| 智能终端快速认证 | 不支持               | * 客户端防破解 | 否       |
| 用户属性类型   |                   | 缺省认证类型   | 网页身份认证  |
| 缺省认证页面   | index_default.jsp |          |         |

确定 取消

## 3.5 验证配置

- (1) 无线用户通过 AP 2 登录 Web，触发 Portal 认证，页面跳转到服务器 IMC 2，用此服务器下配置的用户名密码进行认证。



# 通过 **display wlan client verbose** 命令可以看到，SSID 为 service 的 client 上线。

```
[AC] display wlan client verbose
Total Number of Clients          : 1
Client Information
-----
MAC Address                     : 0021-6a27-97e4
User Name                       : -NA-
AID                             : 1
AP Name                         : officeap2
Radio Id                       : 1
Service Template Number        : 1
SSID                           : service
BSSID                          : 000f-e2e1-5600
Port                            : WLAN-DBSS1:5
VLAN                            : 300
```

# 通过 **display portal user all** 命令可以在 AC 上查看所有 Portal 用户的信息。

```
[AC] display portal user all
Index:2
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC          IP          Vlan  Interface
```

```
-----
0021-6a27-97e4    101.2.0.4          300    Vlan-interface300
Total 1 user(s) matched, 1 listed.
```

# 通过 **display connection** 命令可以在 AC 上查看所有 AAA 用户连接的概要信息。

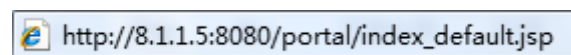
```
[AC] display connection
Index=13    ,Username=lyportal@office2
MAC=00-21-6A-27-97-E4
IP=101.2.0.4
IPv6=N/A
Total 1 connection(s) matched.
```

(2) 无线用户下线，从 AP 1 上线，登录 Web，Portal 认证页面跳转到服务器 IMC 1，用此服务器下配置的用户名密码进行认证。

# 将用户踢下线。

```
[AC] cut connection mac 0021-6a27-97e4
It may take a few seconds or minutes to cut 1 user(s) on the slot 2.
```

# 关闭 AP 2 的 radio，让无线用户从 AP 1 上线，重新进行 Portal 认证，Portal 认证页面正确跳转到服务器 IMC 1 的界面。输入正确的用户名密码通过认证。



# 通过 **display portal user all** 命令可以在 AC 上查看所有 Portal 用户的信息。

```
[AC] display portal user all
Index:16
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC          IP          Vlan    Interface
-----
0021-6a27-97e4    101.2.0.4          300    Vlan-interface300
Total 1 user(s) matched, 1 listed.
```

# 通过 **display connection** 命令可以在 AC 上查看所有 AAA 用户连接的概要信息。

```
[AC] display connection
Index=16    ,Username=lyportal@office1
MAC=00-21-6A-27-97-E4
IP=101.2.0.4
IPv6=N/A
Total 1 connection(s) matched.
```

## 3.6 配置文件

- AC:

```
#
portal server office1 ip 8.1.1.5 key cipher $c$3$qZlb70Wmb3HyL0D7z5kNuGcgPD5QjK5bTi
Q= url http://8.1.1.5:8080/portal server-type imc
portal server office2 ip 8.1.1.40 key cipher $c$3$eo7vKcq64bApp2GeC5X13Ti8T9mu2mU
```

```

+xUA= url http://8.1.1.40:8080/portal server-type imc
portal free-rule 1 source interface GigabitEthernet1/0/1
portal free-rule 2 source ip any destination ip 8.1.1.5 mask 255.255.255.255
portal wlan ssid service spot office1 server office1 domain office1
portal wlan ssid service spot office2 server office2 domain office2
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office1
server-type extended
primary authentication 8.1.1.5
key authentication cipher $c$3$dKnYNS0AR3ECKH7Fy4bL+kSZWNoBoJcTqZU=
user-name-format without-domain
nas-ip 8.101.1.8
#
radius scheme office2
server-type extended
primary authentication 8.1.1.40
key authentication cipher $c$3$k0AxJkrH7bZ3IlH9sfaNrocwoj6j8HuwycM=
user-name-format without-domain
nas-ip 8.101.1.8
#
domain office1
authentication portal radius-scheme office1
authorization portal radius-scheme office1
accounting portal none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
domain office2
authentication portal radius-scheme office2
authorization portal radius-scheme office2
accounting portal none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable

```

```

#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200 300
#
interface Vlan-interface100
 ip address 8.101.1.8 255.255.0.0
#
interface Vlan-interface300
 portal server office2 method direct
 portal domain office2
 portal nas-ip 8.101.1.8
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
#
wlan ap officeap1 model WA2620E-AGN id 1
 serial-id 21023529G007C000020
 radio 2
 service-template 1 vlan-id 300 nas-id office1
 radio enable
#
wlan ap officeap2 model WA2620E-AGN id 2
 serial-id 21023529G007C000021
 radio 2
 service-template 1 vlan-id 300 nas-id office2
 radio enable
#
•   Switch:
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 300
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 poe enable

```

```
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# Portal 支持基于 MAC 地址的快速认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

|                                                  |    |
|--------------------------------------------------|----|
| 1 简介.....                                        | 1  |
| 2 配置前提 .....                                     | 1  |
| 3 配置举例 .....                                     | 1  |
| 3.1 组网需求 .....                                   | 1  |
| 3.2 配置注意事项.....                                  | 2  |
| 3.3 配置步骤 .....                                   | 2  |
| 3.3.1 AC 的配置 .....                               | 2  |
| 3.3.2 Switch 的配置 .....                           | 4  |
| 3.3.3 RADIUS/Portal/MAC trigger server 的配置 ..... | 5  |
| 3.4 验证配置 .....                                   | 12 |
| 3.5 配置文件 .....                                   | 13 |
| 4 相关资料 .....                                     | 15 |

# 1 简介

本文档介绍 Portal 支持基于 MAC 地址的快速认证的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、Portal、WLAN 特性。

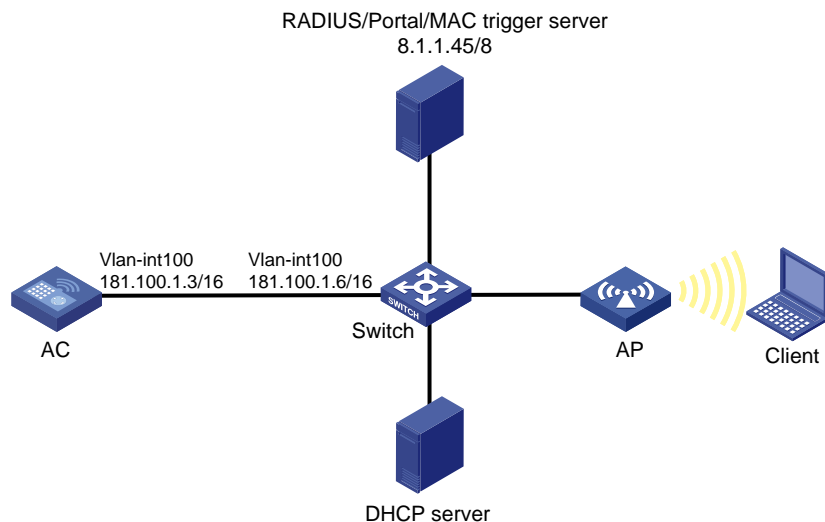
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，AP 和 Client 通过 DHCP 服务器获取 IP 地址，iMC 同时作为 Portal 服务器、RADIUS 服务器和 MAC 绑定服务器，要求：

- Client 在通过 Portal 认证前，只能访问 Portal 服务器；Client 通过 Portal 认证后，可以访问外部网络。
- AC 采用直接方式的 Portal 认证。
- 在 300 秒内，Client 的流量达到 10240 字节之前，允许 Client 访问外部网络资源，一旦流量达到 10240 字节，则触发 MAC 快速认证，不需要用户重新输入用户名和密码。

图1 Portal 支持 MAC 地址的快速认证组网图



## 3.2 配置注意事项

- AC 上配置的 nas-ip 要与 RADIUS 服务器上添加设备时使用的地址一致。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

(1) 配置 AC 的接口。

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 181.100.1.3 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200，作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300，作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口为 Trunk 模式，禁止 VLAN 1 通过，允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] quit
```

# 配置 AC 可达 iMC 的静态路由。

```
[AC] ip route-static 8.0.0.0 255.0.0.0 181.100.1.6
```

(2) 配置无线接口

# 创建 WLAN ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

### (3) 配置无线服务

# 创建 **clear** 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 **SSID** 为 **service**。

```
[AC-wlan-st-1] ssid service
```

# 将 **WLAN-ESS1** 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

### (4) 配置射频接口并绑定服务模板

# 创建 **AP** 的模板，名称为 **officeap**，型号名称选择 **WA2620E-AGN**，并配置 **AP** 的序列号。

```
[AC] wlan ap officeap model WA2620E-AGN
```

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 **radio 2** 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 **AC** 上配置的服务模板 1 与射频 2 进行关联，**Client** 通过服务模板 1 接入 **VLAN 300**。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

# 使能 **AP** 的 **radio 2**。

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

```
[AC-wlan-ap-officeap] quit
```

### (5) 配置 **RADIUS** 方案

# 创建 **RADIUS** 方案 **office** 并进入其视图。

```
[AC] radius scheme office
```

# 服务器类型设置为 **extended**。

```
[AC-radius-office] server-type extended
```

# 设置主认证 **RADIUS** 服务器的 IP 地址 **8.1.1.45**，共享密钥为 **expert**。

```
[AC-radius-office] primary authentication 8.1.1.45 key simple expert
```

# 指定发送给 **RADIUS** 服务器的用户名不携带域名。

```
[AC-radius-office] user-name-format without-domain
```

# 配置 **nas-ip** 为 **VLAN 100** 的地址为 **181.100.1.3**。

```
[AC-radius-office] nas-ip 181.100.1.3
```

```
[AC-radius-office] quit
```

### (6) 配置认证域

# 创建名为 **office** 的域并进入其视图。

```
[AC] domain office
```

# 为 **Portal** 用户配置认证方案为 **RADIUS** 方案，方案名为 **office**。

```
[AC-isp-office] authentication portal radius-scheme office
```

# 为 **Portal** 用户配置授权方案为 **RADIUS** 方案，方案名为 **office**。

```
[AC-isp-office] authorization portal radius-scheme office
```

# 为 **Portal** 用户配置计费为 **none**，不计费。

```
[AC-isp-office] accounting portal none
[AC-isp-office] quit
(7) 配置 Portal 认证
# 配置 Portal 服务器名为 office，地址为 8.1.1.45，密钥为 123456 以及认证页面地址为
http://8.1.1.45:8080/portal。
[AC] portal server office ip 8.1.1.45 key simple 123456 url http://8.1.1.45:8080/portal
# 配置 MAC 绑定服务器的 IP 地址为 8.1.1.45。
[AC] portal mac-trigger server ip 8.1.1.45
# 配置 Portal 免认证规则，符合源接口为 GigabitEthernet1/0/1 的报文不会触发 Portal 认证。
[AC] portal free-rule 0 source interface GigabitEthernet1/0/1
# 进入 VLAN 300 接口视图。
[AC] interface vlan-interface 300
# 配置服务器名为 office，认证方式为直接认证方式。
[AC-Vlan-interface300] portal server office method direct
# 配置 nas-ip 为 181.100.1.3，Portal 认证域为 office。
[AC-Vlan-interface300] portal nas-ip 181.100.1.3
[AC-Vlan-interface300] portal domain office
# 使能 MAC 快速认证功能，指定用户流量的检测周期为 300 秒，触发 MAC 快速认证的流量阈值为 10240 字节。
[AC-Vlan-interface300] portal mac-trigger enable period 300 threshold 10240
[AC-Vlan-interface300] quit
```

### 3.3.2 Switch 的配置

```
# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，
VLAN 300 为无线用户接入的 VLAN。
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] vlan 300
[Switch-vlan300] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 口的 PVID 为
100，允许 VLAN 100、200 和 300 通过。
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 使能 PoE 功能。
```

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 VLAN 100 接口的 IP 地址。
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 181.100.1.6 255.255.0.0
[Switch-Vlan-interface100] quit
```

### 3.3.3 RADIUS/Portal/MAC trigger server 的配置



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.2(E0401)、iMC UAM 5.2(E0402)），说明 RADIUS 服务器的基本配置。

#### (1) 增加接入设备

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[用户接入管理/接入设备管理/接入设备配置/接入设备列表]菜单项，单击<增加>按钮，进入“增加接入设备”页面，单击<手工增加>按钮，进入“手工增加接入设备”页面。

- 填写起始 IP 地址为 181.100.1.3，该 IP 地址为 AC 上配置的 radius scheme 视图下的 nas-ip 地址。
- 单击<确定>按钮完成操作。
- 在“接入配置”页面配置共享密钥为 expert，该共享密钥与 AC 上配置 RADIUS 服务器时的密钥一致。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

业务 >> 用户接入管理 >> 接入设备管理 >> 接入设备配置 >> 增加接入设备

| 接入配置   |              |          |         |
|--------|--------------|----------|---------|
| * 认证端口 | 1812         | * 计费端口   | 1813    |
| * 共享密钥 | *****        | * 确认共享密钥 | *****   |
| 接入区域   | 无            | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 组网方式     | 不启用混合组网 |
| 业务分组   | 未分组          |          |         |

| 设备列表    |             |      |    |    |
|---------|-------------|------|----|----|
| 选择      | 手工增加        | 全部清除 |    |    |
| 共有1条记录。 |             |      |    |    |
| 设备名称    | 设备IP地址      | 设备型号 | 备注 | 删除 |
|         | 181.100.1.3 |      | AC |    |

#### (2) 配置“接入规则管理”

选择“业务”页签，单击导航树中的[用户接入管理/接入规则管理]菜单项，单击<增加>按钮，创建一条接入规则。

- 配置接入规则名为 lyportal（可自定义）。

- 其他采用默认配置。
- 单击<确定>按钮完成。

业务 >> 用户接入管理 >> 接入规则管理 >> 增加接入规则

| 基本信息                                    |                                                                                                   |                                  |   |
|-----------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------|---|
| * 接入规则名                                 | lyportal                                                                                          |                                  |   |
| * 业务分组                                  | 未分组                                                                                               |                                  |   |
| 描述                                      |                                                                                                   |                                  |   |
| 授权信息                                    |                                                                                                   |                                  |   |
| 接入时段                                    | 无                                                                                                 | * 分配IP地址                         | 否 |
| 下行速率                                    |                                                                                                   | 上行速率                             |   |
| 优先级                                     |                                                                                                   | <input type="checkbox"/> 启用RSA认证 |   |
| 证书认证                                    | <input checked="" type="radio"/> 不启用 <input type="radio"/> EAP证书认证 <input type="radio"/> WAPI证书认证 |                                  |   |
| 认证证书类型                                  | EAP-TLS认证                                                                                         |                                  |   |
| 下发VLAN                                  |                                                                                                   |                                  |   |
| <input type="checkbox"/> 下发User Profile |                                                                                                   | 下发用户组                            |   |
| <input type="checkbox"/> 下发ACL          |                                                                                                   |                                  |   |

### (3) 增加服务配置

选择“业务”页签，单击导航树中的[用户接入管理/服务配置管理]菜单项，单击<增加>按钮，创建一条服务。

- 配置服务名为 lyportal（任意命名）。
- 缺省接入规则选择 lyportal。
- 勾选绑定“Portal 智能终端快速认证”。
- 其他选项采用默认配置。
- 单击<确定>按钮完成配置。

业务 >> 用户接入管理 >> 服务配置管理 >> 增加服务配置

| 基本信息                                    |                                                    |          |          |    |    |
|-----------------------------------------|----------------------------------------------------|----------|----------|----|----|
| * 服务名                                   | lyportal                                           | 服务后缀     |          |    |    |
| * 业务分组                                  | 未分组                                                | * 缺省接入规则 | lyportal |    |    |
| * 缺省私有属性下发策略                            | 不使用                                                |          |          |    |    |
| 服务描述                                    |                                                    |          |          |    |    |
| <input checked="" type="checkbox"/> 可申请 | <input checked="" type="checkbox"/> Portal智能终端快速认证 |          |          |    |    |
| 接入策略列表                                  |                                                    |          |          |    |    |
| 增加                                      |                                                    |          |          |    |    |
| 接入场景                                    | 接入规则                                               | 私有属性下发策略 | 优先级      | 修改 | 删除 |
|                                         |                                                    |          |          |    |    |

确定 取消

### (4) 增加接入用户

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户/接入用户列表]菜单项，单击<增加>按钮，增加一个接入用户。

- 单击<选择>按钮，可以选择一个已经存在的用户。

| 接入用户                                         |                                     |                                    |                                     |
|----------------------------------------------|-------------------------------------|------------------------------------|-------------------------------------|
| 接入信息                                         |                                     |                                    |                                     |
| * 用户姓名                                       | <input type="text"/>                | <input type="button" value="选择"/>  | <input type="button" value="增加用户"/> |
| * 帐号名                                        | <input type="text"/>                |                                    |                                     |
| <input type="checkbox"/> 预开用户                | <input type="checkbox"/> 缺省BYOD用户   | <input type="checkbox"/> 主机名用户     | <input type="checkbox"/> 快速认证用户     |
| * 密码                                         | <input type="text"/>                | * 密码确认                             | <input type="text"/>                |
| <input checked="" type="checkbox"/> 允许用户修改密码 | <input type="checkbox"/> 启用用户密码控制策略 | <input type="checkbox"/> 下次登录须修改密码 |                                     |
| 失效日期                                         | <input type="text"/>                | Portal智能终端最大绑定数                    | <input type="text" value="1"/>      |
| 最大闲置时长                                       | <input type="text"/> 分钟             | 在线数量限制                             | <input type="text" value="1"/>      |
| 登录提示信息                                       | <input type="text"/>                |                                    |                                     |

- 或者单击<增加用户>按钮创建一个新用户。

| 接入用户                                         |                                     |                                    |                                     |
|----------------------------------------------|-------------------------------------|------------------------------------|-------------------------------------|
| 接入信息                                         |                                     |                                    |                                     |
| * 用户姓名                                       | <input type="text"/>                | <input type="button" value="选择"/>  | <input type="button" value="增加用户"/> |
| * 帐号名                                        | <input type="text"/>                |                                    |                                     |
| <input type="checkbox"/> 预开用户                | <input type="checkbox"/> 缺省BYOD用户   | <input type="checkbox"/> 主机名用户     | <input type="checkbox"/> 快速认证用户     |
| * 密码                                         | <input type="text"/>                | * 密码确认                             | <input type="text"/>                |
| <input checked="" type="checkbox"/> 允许用户修改密码 | <input type="checkbox"/> 启用用户密码控制策略 | <input type="checkbox"/> 下次登录须修改密码 |                                     |
| 失效日期                                         | <input type="text"/>                | Portal智能终端最大绑定数                    | <input type="text" value="1"/>      |
| 最大闲置时长                                       | <input type="text"/> 分钟             | 在线数量限制                             | <input type="text" value="1"/>      |
| 登录提示信息                                       | <input type="text"/>                |                                    |                                     |

- 输入用户姓名和证件号码，单击<确定>完成。

| 增加用户   |                                 |        |                                     |
|--------|---------------------------------|--------|-------------------------------------|
| 基本信息   |                                 |        |                                     |
| * 用户姓名 | <input type="text" value="ly"/> | * 证件号码 | <input type="text" value="012345"/> |
| 通讯地址   | <input type="text"/>            | 电话     | <input type="text"/>                |
| 电子邮件   | <input type="text"/>            | * 用户分组 | <input type="text" value="未分组"/>    |

|                                   |                                   |
|-----------------------------------|-----------------------------------|
| <input type="button" value="确定"/> | <input type="button" value="取消"/> |
|-----------------------------------|-----------------------------------|

- 配置帐号名和密码，本例中帐号名和密码都为 lyportal。
- 勾选绑定步骤(3)中创建的服务名。
- 单击<确定>按钮完成。



用户 >> 所有接入用户 >> 增加接入用户

### 接入用户

**接入信息**

\* 用户姓名: ly 选择 增加用户

\* 帐号名: lyportal

☐ 预开户用户 ☐ 缺省BYOD用户 ☐ 主机名用户 ☐ 快速认证用户

\* 密码: ..... \* 密码确认: .....

☒ 允许用户修改密码 ☐ 启用用户密码控制策略 ☐ 下次登录须修改密码

失效日期: ..... Portal智能终端最大绑定数: 1

最大闲置时长: ..... 分钟 在线数量限制: 1

登录提示信息: .....

**接入服务**

| 服务名                                          | 服务后缀 | 状态  | 分配IP地址 |
|----------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> lyportal |      | 可申请 |        |

**接入设备绑定信息**

设备序列号: ..... 端口号: .....

外层VLAN ID: .....

## (5) 配置 Portal 主页

选择“业务”页签，单击导航树中的[用户接入管理/Portal 服务管理/服务器配置]菜单项，进入“服务器配置”页面，配置 Portal 主页，采用默认配置即可，单击<确定>按钮完成。

业务 >> 用户接入管理 >> Portal服务管理 >> 服务器配置

### Portal服务器配置

**基本信息**

\* 日志级别: 信息

\* 报文请求超时时长: 4 秒

\* 逃生心跳间隔时长: 20 秒

\* 用户心跳间隔时长: 5 分钟

Portal主页: http://8.1.1.45:8080/portal

## (6) 配置 Portal 认证的地址组范围

选择“业务”页签，单击导航树中的[用户接入管理/Portal 服务管理/IP 地址组配置]菜单项，单击<增加>按钮，配置进行 Portal 认证的地址组范围。

- 配置 IP 地址组名为 ipgroup。
- 配置起始地址为 181.203.0.0。
- 配置终止地址为 181.203.255.255。
- 其他采用默认配置。
- 单击<确定>按钮完成。

| 增加IP地址组  |                 |
|----------|-----------------|
| * IP地址组名 | ipgroup         |
| * IPv6   | 否               |
| * 起始地址   | 181.203.0.0     |
| * 终止地址   | 181.203.255.255 |
| 业务分组     | 未分组             |
| * 类型     | 普通              |

确定 取消

### (7) 配置接入设备信息

选择“业务”页签，单击导航树中的[用户接入管理/Portal 服务管理/设备配置]菜单项，单击<增加>按钮，配置 Portal 认证的接入设备。

- 配置设备名为 AC。
- 配置 IP 地址为 181.100.1.3，该地址与 AC VLAN 300 虚接口下配置的 Portal nas-ip 一致。
- 配置密钥为 123456，该密钥与 AC 上配置 Portal 服务器时设置的密钥一致。
- 其他采用默认配置即可。
- 单击<确定>按钮完成。

| 增加设备信息        |             |
|---------------|-------------|
| 设备信息          |             |
| * 设备名         | AC          |
| * 版本          | Portal 2.0  |
| * 监听端口        | 2000        |
| * 认证重发次数      | 0           |
| * 支持逃生心跳      | 否           |
| * 密钥          | *****       |
| * 组网方式        | 三层          |
| 设备描述          |             |
| * 业务分组        | 未分组         |
| * IP地址        | 181.100.1.3 |
| * 本地Challenge | 否           |
| * 下线重发次数      | 1           |
| * 支持用户心跳      | 否           |
| * 确认密钥        | *****       |

确定 取消

## (8) 配置端口组

返回[用户接入管理/Portal 服务管理/设备配置]菜单项，进入“设备信息列表”，选中设备所在的行，单击“操作”图标，选中<端口组信息管理>按钮，进入“端口组信息配置”页签。



在“端口组信息列表”子页签，单击<增加>按钮，进入到“增加端口组信息”页面。

- 配置端口组名为 portgroup。
- 配置 IP 地址组，选取步骤(6)中创建的地址组 ipgroup。
- “智能终端快速认证”选择“支持”。
- 其他采用默认配置即可。
- 单击<确定>按钮完成。



## (9) 确认终端是否属于智能终端，只有 iMC 支持的智能终端才可以触发无感知 Portal 认证。

选择“业务”页签，单击导航树中的[用户接入管理/终端识别管理]菜单项，检查终端是否符合“终端识别管理”以下六个子菜单标志的特征。

业务 >> 用户接入管理 >> 终端识别管理

加入收藏 帮助

### 终端识别管理简介

终端识别管理用于配置如何根据MAC地址、DHCP特征和HTTP User Agent特征识别终端的厂商、终端类型和操作系统。

iMC可以为不同的终端配置不同的接入策略。当用户使用不同的终端接入网络时，可以获得不同的访问权限。

|                       |                                                                                             |
|-----------------------|---------------------------------------------------------------------------------------------|
| 厂商                    | 终端设备的生产厂家或企业。                                                                               |
| 终端类型                  | 终端设备的类型。                                                                                    |
| 操作系统                  | 终端设备使用的操作系统。                                                                                |
| DHCP特征识别配置            | 用户动态获取IP地址时，DHCP Agent插件会从DHCP请求中将拦截到的终端特征发送到RADIUS服务器。RADIUS服务器通过与iMC系统中DHCP特征进行匹配来识别终端信息。 |
| HTTP User Agent特征识别配置 | 当用户访问iMC页面时，可以通过HTTP请求中携带的User Agent识别终端信息。                                                 |
| MAC地址识别配置             | 用户认证时，RADIUS服务器根据用户的MAC地址与iMC系统中的MAC地址识别配置进行匹配来识别终端信息。                                      |

(10) 对于非智能终端，如 PC 等设备，通常是不进行无感知 Portal 认证的，即每次退出后都要重新进行认证，如果也需要进行无感知 Portal 认证，可对其进行配置。下面以 Windows XP 系统的 PC 为例：

选择“业务”页签，单击导航树中的[用户接入管理/终端识别管理/HTTP User Agent 特征识别配置列表]菜单项，可以发现 Windows XP 系统的 PC 被标志为非智能终端：

业务 >> 用户接入管理 >> 终端识别管理 >> HTTP User Agent特征识别配置

加入收藏 帮助

### HTTP User Agent特征查询

HTTP User Agent特征:  厂商:

终端类型:  操作系统:

智能终端:

查询 重置

### HTTP User Agent特征识别配置列表

增加

共有1条记录，当前第1 - 1，第 1/1 页。 每页显示: 8 15 [50] 100 200

| HTTP User Agent特征 | 厂商        | 终端类型 | 操作系统       | 智能终端 | 描述                        | 修改 | 删除 |
|-------------------|-----------|------|------------|------|---------------------------|----|----|
| Windows NT 5.1    | Microsoft | PC   | Windows XP | 否    | 使用微软公司Windows XP操作系统的个人电脑 |    |    |

- 单击 ，将其修改为智能终端即可。
- 勾选“智能终端”，单击<确定>完成。

### 修改HTTP User Agent特征识别配置

\* HTTP User Agent特征:  ? ☒ 智能终端

厂商:

终端类型:

操作系统:

描述:

确定 取消

### 3.4 验证配置

# 以一个 iOS 5 系统的 iPhone 为例，其符合智能终端的条件。Client 第一次通过 SSID service 上线，获取到 VLAN 300 的地址，此时 Client 只能访问 iMC，无法访问其他地址。

```
[AC] display wlan client
```

```
Total Number of Clients          : 1
                                Client Information
SSID: service
```

| MAC Address    | User Name | APID/RID | IP Address  | VLAN |
|----------------|-----------|----------|-------------|------|
| 00f4-b90d-4220 | -NA-      | 1 / 2    | 181.203.0.3 | 300  |

# 在 Client 的浏览器输入任意地址，如 181.203.1.6，触发 Portal 认证，web 跳转到 <http://8.1.1.45:8080/portal> 页面进行认证，输入用户名和密码，认证成功，Client 能访问该地址，在 AC 上使用 **display connection** 命令和 **display connection ucibindex** 命令看到已经生成了该用户的 Portal 连接表项。

```
[AC] display connection
```

```
Index=11 ,Username=lyportal@office
MAC=00-F4-B9-0D-42-20
IP=181.203.0.3
IPv6=N/A
Online=00h26m44s
Total 1 connection(s) matched.
```

```
[AC] display connection ucibindex 11
```

```
Index=11 , Username=lyportal@office
MAC=00-F4-B9-0D-42-20
IP=181.203.0.3
IPv6=N/A
Access=PORTAL ,AuthMethod=CHAP
Port Type=Wireless-802.11,Port Name=Vlan-interface300
Initial VLAN=300, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Traffic Statistic:
    InputOctets    =0          OutputOctets    =0
    InputGigawords=0          OutputGigawords=0
Priority=Disable
SessionTimeout=N/A, Terminate-Action=N/A
Start=2014-02-11 15:56:15 ,Current=2014-02-11 16:23:34 ,Online=00h27m19s
Total 1 connection matched.
```

# 在终端浏览器的认证窗口点击“下线”，AC 删除 Client 的 Portal 认证表项，此时 Client 已下线。

```
[AC] display connection
```

```
Total 0 connection(s) matched.
```

# Client 再次通过浏览器访问 181.203.1.6 时，不会再跳转到 Portal 认证页面就可以直接访问该地址，从而实现了 Portal 快速认证。此时，AC 和 RADIUS 服务器上重新生成了 Client 的连接表项。

```
[AC] display connection
```

```
Index=12 ,Username=lyportal@office
```

```
MAC=00-F4-B9-0D-42-20
```

```
IP=181.203.0.3
```

```
IPv6=N/A
```

```
Total 1 connection(s) matched.
```

```
[AC] display connection ucibindex 12
```

```
Index=12 , Username=lyportal@office
```

```
MAC=00-F4-B9-0D-42-20
```

```
IP=181.203.0.3
```

```
IPv6=N/A
```

```
Access=PORTAL ,AuthMethod=CHAP
```

```
Port Type=Wireless-802.11,Port Name=Vlan-interface300
```

```
Initial VLAN=300, Authorization VLAN=N/A
```

```
ACL Group=Disable
```

```
User Profile=N/A
```

```
CAR=Disable
```

```
Priority=Disable
```

```
SessionTimeout=86155(s), Terminate-Action=Default
```

```
Start=2014-2-11 16:50:44 ,Current=2014-2-11 16:54:51 ,Online=00h04m07s
```

```
Total 1 connection matched.
```

## 3.5 配置文件

- AC:

```
#
```

```
portal server office ip 8.1.1.45 key cipher $c$3$6834TPQFh7IQFVzINGf5YpGmL6t/vM
```

```
SF8A== url http://8.1.1.45:8080/portal
```

```
portal free-rule 0 source interface GigabitEthernet1/0/1
```

```
portal mac-trigger server ip 8.1.1.45
```

```
#
```

```
vlan 100
```

```
#
```

```
vlan 200
```

```
#
```

```
vlan 300
```

```
#
```

```
radius scheme office
```

```
server-type extended
```

```
primary authentication 8.1.1.45 key cipher $c$3$z1EqZpP4E2oWMP0h3EEGRr5fZTW580H
```

```
LKg==
```

```
user-name-format without-domain
```

```
nas-ip 181.100.1.3
```

```
#
```

```
domain office
```

```

authentication portal radius-scheme office
authorization portal radius-scheme office
accounting portal none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200 300
#
interface Vlan-interface100
  ip address 181.100.1.3 255.255.0.0
#
interface Vlan-interface300
  portal server office method direct
  portal domain office
  portal nas-ip 181.100.1.3
  portal mac-trigger enable period 300 threshold 10240
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
    service-template 1 vlan-id 300
  radio enable
#
ip route-static 8.0.0.0 255.0.0.0 181.100.1.6
#
●    Switch:
#
vlan 100
#
vlan 200

```

```
#
vlan 300
#
interface Vlan-interface100
 ip address 181.100.1.6 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200 300
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。



# H3C 无线控制器 Portal MAC-Trigger IPv6 自动认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                       |    |
|-----------------------|----|
| 1 简介.....             | 1  |
| 2 配置前提 .....          | 1  |
| 3 配置举例 .....          | 1  |
| 3.1 组网需求 .....        | 1  |
| 3.2 配置思路 .....        | 2  |
| 3.3 配置注意事项.....       | 2  |
| 3.4 配置步骤 .....        | 2  |
| 3.4.1 配置 iMC .....    | 2  |
| 3.4.2 配置 AC.....      | 10 |
| 3.4.3 配置 Switch ..... | 13 |
| 3.5 验证配置 .....        | 14 |
| 3.6 配置文件 .....        | 15 |
| 4 相关资料 .....          | 17 |

# 1 简介

本文档介绍 Portal MAC-Trigger IPv6 自动认证配置举例。

## 2 配置前提

本文档不严格与具体硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、Portal、WLAN 特性。

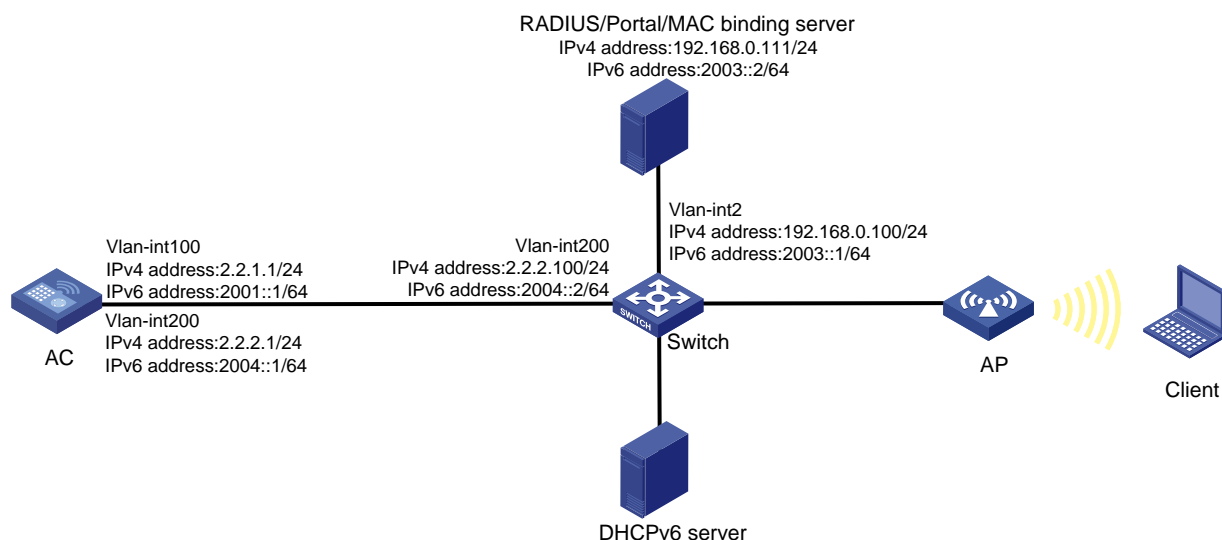
## 3 配置举例

### 3.1 组网需求

如图 1 所示，AP 和 Client 通过 DHCP 和 DHCPv6 服务器获取 IP 和 IPv6 地址，iMC 同时作为 Portal 认证服务器和 Portal Web 服务器、RADIUS 服务器和 MAC 绑定服务器，要求：

- Client 在通过 Portal 认证前，只能访问 Portal Web 服务器；Client 通过 Portal 认证后，可以访问外部网络。
- 在 Client 的流量达到 1024000 字节之前，允许 Client 访问外部网络资源，一旦流量达到 1024000 字节，则触发 MAC 快速认证。

图1 Portal MAC-Trigger IPv6 自动认证组网图



## 3.2 配置思路

- 为了通过 MAC-Trigger 实现 IPv6 自动认证，AC、Client 和 iMC 需要同时配置 IPv4 和 IPv6 地址，且各设备间 IPv4 路由和 IPv6 路由都需要可达。
- 为了将 AP 的 GigabitEthernet1/0/1 接口加入本地转发的 VLAN 200，需要使用文本文档编辑 AP 的配置文件，并将配置文件上传到 AC 存储介质上。
- 为了防止用户上线过程中，动态授权信息下发失败，需要配置 RADIUS DAE 服务器功能。
- 为了使用户通过一次 Portal 认证既能访问 IPv4 网络也能访问 IPv6 网络，需要开启 Portal 支持双协议栈功能。
- 为了在 AC 上查看用户 IPv6 地址，需要开启通过 DHCPv6 方式学习客户端 IPv6 地址功能和通过 ND 方式学习客户端 IPv6 地址功能。
- 如果需要域名解析，请增加 DNS 相关配置，本举例略。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- AC 上配置的 Portal 认证服务器、Portal Web 服务器和 MAC 绑定服务器的服务器类型必须与实际服务器一致。
- 若在 VLAN 接口视图下开启 Portal 认证，只能采用集中转发；若在服务模板视图下开启 Portal 认证，则本地转发和集中式转发都支持。
- 配置用户免认证流量的阈值后，客户端不会自动弹出 Portal 认证页面，需要手动打开浏览器进行重定向，如果希望自动弹出 Portal 认证页面，请不要配置该阈值。

## 3.4 配置步骤

### 3.4.1 配置 iMC



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.1(E0303)、iMC EIA 7.1(E0304)、iMC EIP 7.1(E0304)）说明 RADIUS server、Portal server 和 MAC 绑定服务器的基本配置。

#### (1) 配置 RADIUS server

##### # 增加接入设备

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，单击<增加>按钮，进入“增加接入设备”页面。

- 配置共享密钥为 radius，该共享密钥与 AC 上配置 RADIUS 服务器时的密钥一致。
- 单击<手工增加>按钮，进入“手工增加接入设备”页面，填写起始 IP 地址为 2.2.2.1，单击<确定>按钮完成操作。

- 单击<增加 IPv6 设备>按钮，进入“手工增加接入设备”页面，填写起始 IP 地址为 2001::1，单击<确定>按钮完成操作。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

图2 增加 IPv4 接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

接入配置

|        |              |          |         |
|--------|--------------|----------|---------|
| 认证端口 * | 1812         | 计费端口 *   | 1813    |
| 组网方式   | 不启用混合组网      | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 业务分组     | 未分组     |
| 共享密钥 * | *****        | 确认共享密钥 * | *****   |
| 接入设备分组 | 无            |          |         |

设备列表

选择 手工增加 增加IPv6设备 全部清除

| 设备名称 | 设备IP地址  | 设备型号 | 备注 | 删除 |
|------|---------|------|----|----|
|      | 2.2.2.1 |      |    | 删除 |

共有1条记录。

确定 取消

图3 增加 IPv6 接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

接入配置

|        |              |          |         |
|--------|--------------|----------|---------|
| 认证端口 * | 1812         | 计费端口 *   | 1813    |
| 组网方式   | 不启用混合组网      | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 业务分组     | 未分组     |
| 共享密钥 * | *****        | 确认共享密钥 * | *****   |
| 接入设备分组 | 无            |          |         |

设备列表

选择 手工增加 增加IPv6设备 全部清除

| 设备名称 | 设备IP地址                                  | 设备型号 | 备注 | 删除 |
|------|-----------------------------------------|------|----|----|
|      | 2001:0000:0000:0000:0000:0000:0000:0001 |      |    | 删除 |

共有1条记录。

确定 取消

## (2) 配置 Portal server

### # 配置 Portal 认证服务

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面。

- 根据实际组网情况调整以下参数，本例中使用缺省配置。

图4 Portal 认证服务器配置页面

用户 > 接入策略管理 > Portal服务管理 > 服务器配置

Portal服务器配置

基本信息

日志级别 \*

信息

Portal Server

报文请求超时时长(秒) \*

4

⑦

逃生心跳间隔时长(秒) \*

20

⑦

用户心跳间隔时长(分钟) \*

5

⑦

LB设备地址

LB设备IPv6地址

Portal Web

请求报文超时时长(秒) \*

15

⑦

交互报文编码

⑦

校验终端用户请求报文

是

⑦

使用缓存

是

⑦

HTTP心跳界面展示方式

新页面

⑦

HTTPS心跳界面展示方式

原页面

⑦

Portal主页

http://192.168.100.240:8080/portal/  
http://192.168.100.240:8443/portal/  
http://[2003::2]:8080/portal/  
https://[2003::2]:8443/portal/

高级信息

服务类型列表

增加

共有0条记录。

| 服务类型标识      | 服务类型 | 删除 |
|-------------|------|----|
| 未找到符合条件的记录。 |      |    |

确定

# 配置 IP 地址组。

单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入 Portal IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名；
- IPv6 选择“是”。（仅 IPv6，IPv4 地址选“否”）
- 输入起始地址和终止地址，输入的地址范围中应包含用户主机的 IP 地址；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。（仅 IPv4 地址组配置本项）

图5 增加 IPv4 地址组配置页面

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组

增加IP地址组

|          |             |
|----------|-------------|
| IP地址组名 * | Portal_user |
| 起始地址 *   | 2.2.2.1     |
| 终止地址 *   | 2.2.2.255   |
| 业务分组     | 未分组         |
| 类型 *     | 普通          |

确定 取消

图6 增加 IPv6 地址组配置页面

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组

增加IP地址组

|          |               |
|----------|---------------|
| IP地址组名 * | Portal_userv6 |
| IPv6 *   | 是             |
| 起始地址 *   | 2004::1       |
| 终止地址 *   | 2004::255     |
| 业务分组     | 未分组           |

确定 取消

#### # 增加 Portal 设备

单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；
- IPv4 用户版本选择“Portal 2.0”，IPv6 用户版本选择“Portal 3.0”；
- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 选择是否支持逃生心跳功能和用户心跳功能，本例中选择否。
- 输入密钥，与 AC 上的配置保持一致；
- 选择组网方式为直连；
- 其它参数可采用缺省配置。

图7 增加 IPv4 设备信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

增加设备信息

设备信息

设备名 \*

NAS

版本 \*

Portal 2.0

监听端口 \*

2000

认证重发次数 \*

0

支持逃生心跳 \*

否

密钥 \*

\*\*\*\*\*

组网方式 \*

直连

设备描述

业务分组 \*

未分组

IP地址 \*

2.2.2.1

本地Challenge \*

否

下线重发次数 \*

1

支持用户心跳 \*

否

确认密钥 \*

\*\*\*\*\*

确定

取消

图8 增加 IPv6 设备信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

增加设备信息

设备信息

设备名 \*

NASv6

版本 \*

Portal 3.0

监听端口 \*

2000

认证重发次数 \*

0

支持逃生心跳 \*

否

密钥 \*

\*\*\*\*\*

组网方式 \*

直连

设备描述

业务分组 \*

未分组

IP地址 \*

2004::1

本地Challenge \*

否

下线重发次数 \*

1

支持用户心跳 \*

否

确认密钥 \*

\*\*\*\*\*

确定

取消

# Portal 设备关联 IP 地址组

在 Portal 设备配置页面中的设备信息列表中，单击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图9 IPv4 设备信息列表

用户 > 接入策略管理 > Portal服务管理 > 设备配置

★加入收藏 ②帮助

设备信息查询

设备名

版本

下发结果

业务分组

查询

重置

增加

| 设备名 | 版本         | 业务分组 | IP地址    | IPv6地址 | 最近一次下发时间 | 下发结果 | 操作          |
|-----|------------|------|---------|--------|----------|------|-------------|
| NAS | Portal 2.0 | 未分组  | 2.2.2.1 |        |          | 未下发  | <div></div> |

共有1条记录，当前第1-1，第 1/1 页。

<<

<

1

>

>>

50



图10 IPv6 设备信息列表

设备信息查询

设备名

下发结果

版本

业务分组

查询

重置

| 设备名   | 版本         | 业务分组 | IP地址 | IPv6地址 | 最近一次下发时间 | 下发结果 | 操作                                                                                                                                                                                                                                                          |
|-------|------------|------|------|--------|----------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NASv6 | Portal 3.0 | 未分组  |      | 2004:1 |          | 未下发  |    |

在端口组信息配置页面中单击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 无感知认证选择“支持”；
- 其它参数可采用缺省配置。

图11 增加端口组信息配置页面

增加端口组信息

端口组名 \*

group

开始端口 \*

0

协议类型 \*

HTTP

是否NAT \*

否

认证方式 \*

PAP认证

心跳间隔(分钟) \*

0

用户域名

无感知认证

支持

页面推送策略

提示信息 \*

动态检测

终止端口 \*

zzzzzz

快速认证 \*

否

错误速传 \*

是

IP地址组 \*

Portal\_user

心跳超时(分钟) \*

0

端口组描述

客户端防破解 \*

否

缺省认证页面

确定

取消

图12 增加 IPv6 端口组信息配置页面

增加端口组信息

端口组名 \*

groupv6

开始端口 \*

0

协议类型 \*

HTTP

是否NAT \*

否

认证方式 \*

PAP认证

心跳间隔(分钟) \*

0

用户域名

无感知认证

支持

页面推送策略

提示信息 \*

动态检测

终止端口 \*

zzzzzz

快速认证 \*

否

错误速传 \*

是

IP地址组 \*

Portal\_userv6

心跳超时(分钟) \*

0

端口组描述

客户端防破解 \*

否

缺省认证页面

确定

取消

# 最后单击导航树中的[接入策略管理/业务参数配置/系统配置手工生效]菜单项，使以上 Portal 认证服务器配置生效。

(3) 配置 MAC 绑定服务器

# 增加接入策略

单击导航树中的[接入策略管理/接入策略管理]菜单项，并单击<增加>按钮，进入“增加接入策略”页面。

- 填写接入策略名；
- 选择业务分组；
- 其它参数可采用缺省配置。

图13 增加接入策略配置

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

**基本信息**

接入策略名 \* AccessPolicy

业务分组 \* 未分组

描述

**授权信息**

接入时段 无

下行速率(Kbps)

优先级

证书认证 ☒ 不启用 ☐ EAP证书认证 ☐ WAPI证书认证

认证证书类型 EAP-TLS认证

下发VLAN

☐ 下发User Profile

☐ 下发ACL

分配IP地址 \* 否

上行速率(Kbps)

☐ 启用RSA认证

下发用户组

## # 增加接入服务

单击导航树中的[接入策略管理/接入服务管理]菜单项，并单击<增加>按钮，进入“增加接入服务配置”页面。

- 填写服务名；
- 缺省接入策略选择已配置好的接入策略；
- 勾选“Portal 无感知认证”；
- 其它参数可采用缺省配置。

图14 增加接入服务配置

用户 > 接入策略管理 > 接入服务管理 > 修改接入服务

**基本信息**

服务名 \* MAC\_server

业务分组 \* 未分组

缺省私有属性下发策略 \* 不使用

缺省单帐号最大绑定终端数 \* 0

服务描述

☒ 可申请

服务后缀

缺省接入策略 \* AccessPolicy

缺省单帐号在线数量限制 \* 0

☒ Portal无感知认证

## # 增加接入用户

单击导航树中的[接入用户管理/接入用户]菜单项，并单击<增加>按钮，进入增加接入用户页面。

- 用户姓名选择已经存在的可接入的用户或单击<增加用户按钮>，增加一个新用户；
- 填写账号名；
- 设置密码；
- 设置“Portal 无感知认证最大绑定数”；
- 其它参数可采用缺省配置。

图15 增加接入用户

用户 > 接入用户 > 增加接入用户

接入用户

接入信息

用户姓名 \* Client1 选择 增加用户

帐号名 \* Client

☐ 预开户用户 ☐ 缺省BYOD用户 ☐ MAC地址认证用户 ☐ 主机名用户 ☐ 快速认证用户

密码 \* ..... 密码确认 \* .....

☒ 允许用户修改密码 ☐ 启用用户密码控制策略 ☐ 下次登录须修改密码

生效时间 ..... 失效时间 .....

最大闲置时长(分钟) ..... 在线数量限制 1

Portal无感知认证最大绑定数 5

登录提示信息

## # 配置系统参数

单击导航树中的[接入策略管理/业务参数配置/系统配置]菜单项，并单击[终端管理参数配置]对应的<配置>按钮，进入终端管理参数配置页面。

- 无感知认证选择“启用”；
- “非智能终端 Portal 无感知认证”可根据实际需要允许或禁用，本例中为允许。

图16 配置终端管理参数

用户 > 接入策略管理 > 业务参数配置 > 系统配置 > 终端管理参数配置

终端管理参数配置

无感知认证 启用

非智能终端Portal无感知认证 允许

单帐号最多绑定终端数 \* 10

终端信息不一致时强制下线 否

确定 取消

单击导航树中的[接入策略管理/业务参数配置/系统配置]菜单项，单击[终端老化时长]对应的<配置>按钮，然后单击<修改>，进入终端老化时长配置页面。

根据实际需要配置终端老化时间，本例中采用默认值。

图17 配置终端老化时长



用户 > 接入策略管理 > 业务参数配置 > 系统配置 > 终端老化时长配置 > 修改终端老化时长

修改终端老化时长

终端老化时长(天) \*  ?

确定 取消

# 最后单击导航树中的[接入策略管理/业务参数配置/系统配置手工生效]菜单项，使以上配置生效。

### 3.4.2 配置 AC

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。AP 将通过该 VLAN 与 AC 建立 CAPWAP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] ipv6 address 2001::1 64
```

# 取消对 RA 消息发布的抑制。

```
[AC-Vlan-interface100] undo ipv6 nd ra halt
```

# 设置被管理地址配置标志位为 1。

```
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

# 设置其他配置标志位为 1。

```
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。Client 将使用该 VLAN 接入无线网络。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] ipv6 address 2004::1 64
```

# 取消对 RA 消息发布的抑制。

```
[AC-Vlan-interface200] undo ipv6 nd ra halt
```

# 设置被管理地址配置标志位为 1。

```
[AC-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
```

# 设置其他配置标志位为 1。

```
[AC-Vlan-interface200] ipv6 nd autoconfig other-flag
```

```
[AC-Vlan-interface200] quit
```

## (2) 配置无线接口

# 创建 WLAN ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

## (3) 配置静态路由

# 配置到 iMC 服务器的静态路由。

```
[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

```
[AC] ipv6 route-static 2003:: 64 2004::2
```

## (4) 配置无线服务

# 创建无线服务模板 1，并进入无线服务模板视图。

```
[AC] wlan service-template 1 clear
```

# 配置 SSID 为 service。

```
[AC-wlan-st-st1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

# 创建 AP，配置 AP 名称为 office，型号名称选择 WA2620E-AGN，并配置序列号 21023529G007C000020。

```
[AC] wlan ap office model WA2620E-AGN
```

```
[AC-wlan-ap-office] serial-id 21023529G007C000020
```

# 进入 Radio 2 视图。

```
[AC-wlan-ap-office] radio 2
```

# 将无线服务模板 1 绑定到 radio 2，设置绑定到射频接口的 VLAN 编号为 VLAN 200，并开启射频。

```
[AC-wlan-ap-office-radio-2] service-template 1 vlan-id 200
```

```
[AC-wlan-ap-office-radio-2] radio enable
```

```
[AC-wlan-ap-office-radio-2] quit
```

```
[AC-wlan-ap-office] quit
```

## (5) 配置 IPv4 RADIUS 方案

# 创建名称为 rs1 的 RADIUS 方案，并进入该方案视图。

```
[AC] radius scheme rs1
```

# 配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[AC-radius-rs1] primary authentication 192.168.0.111
[AC-radius-rs1] primary accounting 192.168.0.111
[AC-radius-rs1] key authentication simple radius
[AC-radius-rs1] key accounting simple radius
# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。
[AC-radius-rs1] user-name-format without-domain
# 设置设备发送 RADIUS 报文使用的源 IP 地址为 2.2.2.1。
[AC-radius-rs1] nas-ip 2.2.2.1
[AC-radius-rs1] quit
```

#### (6) 配置 IPv6 RADIUS 方案

```
# 创建名称为 rs2 的 RADIUS 方案，并进入该方案视图。
[AC] radius scheme rs2
# 配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。
[AC-radius-rs2] primary authentication ipv6 2003::2
[AC-radius-rs2] primary accounting ipv6 2003::2
[AC-radius-rs2] key authentication simple radius
[AC-radius-rs2] key accounting simple radius
# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。
[AC-radius-rs2] user-name-format without-domain
# 设置设备发送 RADIUS 报文使用的源 IPv6 地址为 2004::1。
[AC-radius-rs1] nas-ip ipv6 2004::1
[AC-radius-rs2] quit
```

#### (7) 配置 IPv4 用户认证域

```
# 创建名为 dm1 的 ISP 域并进入其视图。
[AC] domain dm1
# 为 Portal 用户配置 AAA 认证方法为 RADIUS。
[AC-isp-dm1] authentication portal radius-scheme rs1
# 为 Portal 用户配置 AAA 授权方法为 RADIUS。
[AC-isp-dm1] authorization portal radius-scheme rs1
# 为 Portal 用户配置 AAA 计费方法为 none，不计费。
[AC-isp-dm1] accounting portal none
[AC-isp-dm1] quit
```

#### (8) 配置 IPv6 用户认证域

```
# 创建名为 dm2 的 ISP 域并进入其视图。
[AC] domain dm2
# 为 Portal 用户配置 AAA 认证方法为 RADIUS。
[AC-isp-dm2] authentication portal radius-scheme rs2
# 为 Portal 用户配置 AAA 授权方法为 RADIUS。
[AC-isp-dm2] authorization portal radius-scheme rs2
# 为 Portal 用户配置 AAA 计费方法为 none，不计费。
[AC-isp-dm2] accounting portal none
[AC-isp-dm2] quit
```

#### (9) 配置 Portal 认证

# 配置 IPv4 Portal 认证服务器，名称为 newptv4，IP 地址为 192.168.0.111，密钥为 123456 以及认证页面地址为 http://192.168.0.111:8080/portal。。

```
[AC] portal server newptv4 ip 192.168.0.111 key simple 123456 url
http://192.168.0.111:8080/portal
```

# 配置 IPv6 Portal 认证服务器，名称为 newptv6，IPv6 地址为 2003::2。

```
[AC] portal server newptv6 ipv6 2003::2 key simple 123456 url http://[2003::2]:8080/portal
```

# 在 VLAN200 接口上使能直接方式的 Portal 认证。

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] portal server newptv4 method direct
[AC-Vlan-interface200] portal server newptv6 method direct
```

# 配置接入的 IPv4 Portal 用户使用认证域为 dm1。

```
[AC-Vlan-interface200] portal domain dm1
```

# 配置接入的 IPv6 Portal 用户使用认证域为 dm2。

```
[AC-Vlan-interface200] portal domain ipv6 dm2
```

# 配置用户免认证流量的阈值为 1024000 字节。

```
[AC-Vlan-interface200] portal mac-trigger enable threshold 1024000
```

# 配置 Portal 用户报文的控制模式为 MAC。

```
[AC-Vlan-interface200] portal control-mode mac
```

# 设置发送给 Portal 认证服务器的 Portal 报文中的 BAS-IP 和 BAS-IPv6 属性。

```
[AC-Vlan-interface200] portal bas-ip 2.2.2.1
[AC-Vlan-interface200] portal bas-ipv6 2004::1
[AC-Vlan-interface200] quit
```

#### (10) 配置 Portal 基于 MAC 地址的快速认证

# 配置 MAC 绑定服务器的 IP 地址为 192.168.0.111。

```
[AC] portal mac-trigger server ip 192.168.0.111
```

### 3.4.3 配置 Switch

# 创建 VLAN 100，用于转发 AC 和 AP 间 CAPWAP 隧道内的流量。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# 创建 VLAN 200，用于转发 Client 无线报文。

```
[Switch] vlan 200
[Switch-vlan200] quit
```

# 创建 VLAN 2。

```
[Switch] vlan 2
[Switch-vlan2] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 VLAN 200 接口的 IP 地址和 IPv6 地址。
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] ipv6 address 2004::2 64
[Switch-Vlan-interface200] quit
# 配置 VLAN 2 接口的 IP 地址和 IPv6 地址。
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] ipv6 address 2003::1 64
[Switch-Vlan-interface2] quit
```

### 3.5 验证配置

# 用户通过网页方式进行 Portal 认证。用户在通过认证前，发起的所有 Web 访问均被重定向到 Portal 认证页面(<http://192.168.0.111:8080/portal>)，在通过认证后，可访问非受限的互联网资源。用户在首次进行 Portal 认证时，需要手工输入用户名和密码。当用户再次上线时，将可以直接访问互联网资源，不会感知到 Portal 认证过程。

通过执行以下显示命令查看 AC 上生成的 Portal 在线用户信息。

```
[AC] display portal user all verbose
Total portal users: 1
Basic:
  AP name: office
  Radio ID: 1
  SSID: service
  Current IP address: 163.200.0.13
  Original IP address: 163.200.0.13
  Username: 4C:49:E3:F8:CC:9D
  User ID: 0x1000002d
  Access interface: WLAN-BSS1/0/17
  Service-VLAN/Customer-VLAN: 200/-
  MAC address: 4c49-e3f8-cc9d
  Authentication type: MAC-trigger
  Domain name: dm
  VPN instance: N/A
  Status: Online
  Portal server: newpt
  Vendor: Xiaomi
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 720s, retry times: 5
  Idle cut: N/A
```



```

Session duration: 86400 sec, remaining: 86385 sec
Remaining traffic: N/A
Login time: 2018-08-10 17:13:58 Beijing
Online time(hh:mm:ss): 00:00:15
DHCP IP pool: N/A
ACL&QoS&Multicast:
  Inbound CAR: N/A
  Outbound CAR: N/A
  ACL number: N/A
  User profile: N/A
  Session group profile: N/A
  Max multicast addresses: 4
Flow statistic:
  Uplink   packets/bytes: 18/5595
  Downlink packets/bytes: 18/1971
Dual stack flow statistic:
  Ipv4 address: 163.105.0.13
        uplink   packets/bytes: 18/5595
        downlink packets/bytes: 18/1971
  Ipv6 address: 2004::2
        uplink   packets/bytes: 0/0
        downlink packets/bytes: 0/0

```

## 3.6 配置文件

- AC:
 

```

#
portal server newptv4 ip 192.168.0.111 key cipher $c$3$HBHc6HSMkLMDlu+IqMznbtUx
mjew7M/ESA== url http://192.168.0.111:8080/portal server-type imc
portal server newptv6 ipv6 2003::2 key cipher $c$3$9JwQ7cpuGX/eN3oSU4eCSWp1FT6L
wkYR5Q== url http://[2003::2]:8080/portal server-type imc
portal mac-trigger server ip 192.168.0.111
#
vlan 100
#
vlan 200
#
radius scheme rs1
  primary authentication 192.168.0.111
  primary accounting 192.168.0.111
  key authentication cipher $c$3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
  key accounting cipher $c$3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
  user-name-format without-domain
  nas-ip 2.2.2.1
radius scheme rs2
  primary authentication ipv6 2003::0002
  primary accounting ipv6 2003::0002
  key authentication cipher $c$3$ZqzlvbN5k1p/VDqt/prrN97yy0J4G2j8IQ==

```

```

key accounting cipher $c$3$Q6Noroq7nFDkIBYIvpIZu3qQpAZzaDUYJQ==
user-name-format without-domain
nas-ip ipv6 2004::1
#
domain dml
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal none
access-limit disable
state active
idle-cut disable
self-service-url disable
domain dm2
authentication portal radius-scheme rs2
authorization portal radius-scheme rs2
accounting portal none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
ipv6 address 2001::1/64
ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
ipv6 address 2004::1/64
ip address 2.2.2.1 255.255.255.0
portal control-mode mac
portal server newptv4 method direct
portal server newptv6 method direct
portal domain dml
portal bas-ip 2.2.2.1
portal domain ipv6 dm2
portal bas-ipv6 2004::1
portal mac-trigger enable threshold 1024000
#

```

```

interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap office model WA2620E-AGN id 2
  serial-id 21023529G007C000020
  radio 1
  radio 2
  service-template 1 vlan-id 200
  radio enable
#
•   Switch:
#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
  ip address 192.168.0.100 255.255.255.0
  ipv6 address 2003::1 64
#
interface Vlan-interface200
  ip address 2.2.2.100 255.255.255.0
  ipv6 address 2004::2 64
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”

# 本地 Portal 认证基于 SSID 绑定认证页面典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                               |    |
|-------------------------------|----|
| 1 简介.....                     | 1  |
| 2 配置前提 .....                  | 1  |
| 3 配置举例 .....                  | 1  |
| 3.1 组网需求 .....                | 1  |
| 3.2 配置思路 .....                | 1  |
| 3.3 配置注意事项.....               | 1  |
| 3.4 配置步骤 .....                | 2  |
| 3.4.1 AC 的配置 .....            | 2  |
| 3.4.2 Switch 的配置 .....        | 4  |
| 3.4.3 RADIUS server 的配置 ..... | 5  |
| 3.5 验证配置 .....                | 8  |
| 3.6 配置文件 .....                | 9  |
| 4 相关资料 .....                  | 11 |

# 1 简介

本文档介绍本地 Portal 认证基于 SSID 绑定认证页面的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、WLAN 无线接入、Portal 认证特性。

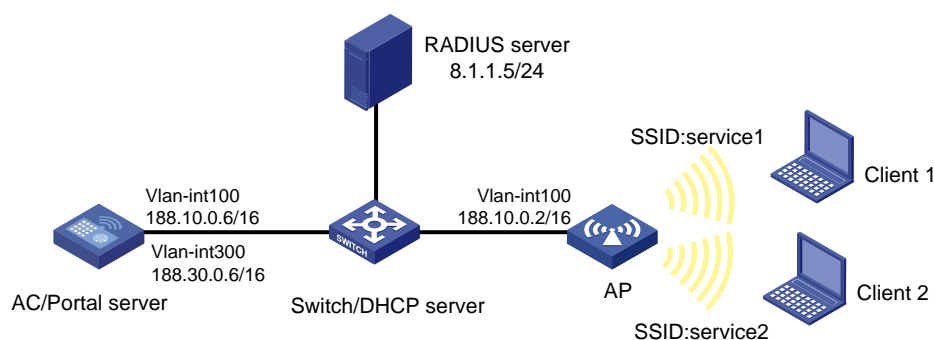
## 3 配置举例

### 3.1 组网需求

如图 1 所示，RADIUS 服务器作为认证/计费服务器，Switch 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址。要求通过基于 SSID 绑定本地 Portal 认证页面的功能，实现：

- 当无线客户端通过名为 service1 的 SSID 接入网络时，Portal 认证推出自定义的认证页面；
- 当无线客户端通过名为 service2 的 SSID 接入网络时，Portal 认证推出的是系统默认认证页面。

图1 本地 Portal 认证基于 SSID 绑定认证页面组网图



### 3.2 配置思路

为了使无线客户端从 service1 接入时推出自定义认证页面，需编辑自定义认证页面并上传至 AC。

### 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 188.10.0.6 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并配置其接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 188.30.0.6 16
[AC-Vlan-interface300] quit
```

# 配置 AC 连接 Switch 的 GigabitEthernet1/0/1 接口的属性为 trunk，并允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置认证策略和认证域

# 在 AC 上创建 RADIUS 方案 office 并进入其视图。

```
[AC] radius scheme office
```

# 配置 RADIUS 方案的主认证服务器及其通信密钥。

```
[AC-radius-office] primary authentication 8.1.1.5
[AC-radius-office] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC-radius-office] user-name-format without-domain
[AC-radius-office] quit
```

# 配置发送 RADIUS 报文的源 IP 地址为 188.10.0.6。

```
[AC] radius nas-ip 188.10.0.6
```

# 创建并进入名字为 office 的 ISP 域视图。

```
[AC] domain office
```

# 为 Portal 用户配置 AAA 认证方法为 RADIUS 认证/授权方案 office，不计费。

```
[AC-isp-office] authentication portal radius-scheme office
[AC-isp-office] authorization portal radius-scheme office
[AC-isp-office] accounting portal none
```

### (3) 配置 Portal

# 配置 Portal 服务器：名称为 office，IP 地址为 188.10.0.6。

```
[AC] portal server office ip 188.10.0.6
```

# 配置本地 Portal 服务器支持 HTTP 协议。

```
[AC] portal local-server http
```

# 在用户所在的 VLAN 300 接口上使能 Portal。

```
[AC] interface vlan-interface 300
```

```
[AC-Vlan-interface300] portal server office method direct
```

# 指定 Portal 用户的认证域为 office。

```
[AC-Vlan-interface300] portal domain office
```

```
[AC-Vlan-interface300] quit
```

### (4) 配置 WLAN 服务

# 创建接口 WLAN-ESS 1，并设置端口的链路类型为 Hybrid。

```
[AC] interface wlan-ess 1
```

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

# 创建接口 WLAN-ESS 2，并设置端口的链路类型为 Hybrid。

```
[AC] interface wlan-ess 2
```

```
[AC-WLAN-ESS2] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS2] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS2] port hybrid vlan 200 untagged
```

```
[AC-WLAN-ESS2] port hybrid pvid vlan 200
```

```
[AC-WLAN-ESS2] mac-vlan enable
```

```
[AC-WLAN-ESS2] quit
```

# 配置 WLAN 服务模板 1，SSID 为 service1，并将接口 WLAN-ESS 1 与该服务模板绑定，启用无线服务。

```
[AC] wlan service-template 1 clear
```

```
[AC-wlan-st-1] ssid service1
```

```
[AC-wlan-st-1] bind wlan-ess 1
```

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

# 配置 WLAN 服务模板 2，SSID 为 service2，并将接口 WLAN-ESS 2 与该服务模板绑定，启用无线服务。

```
[AC] wlan service-template 2 clear
```

```
[AC-wlan-st-2] ssid service2
```

```
[AC-wlan-st-2] bind wlan-ess 2
```

```
[AC-wlan-st-2] service-template enable
```

```
[AC-wlan-st-2] quit
```

# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN，并配置 AP 的序列号。



```
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将服务模板 1 和 2 绑定到 AP 的 Radio 2 口，配置绑定到 Radio 2 口的 VLAN 为 VLAN 300，并使
能 Radio 2。
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
[AC-wlan-ap-officeap-radio-2] service-template 2 vlan-id 300
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

#### (5) 将自定义认证页面文件上传至 AC

# 通过 FTP 将本地的自定义认证页面文件 **ssid1.zip** 上传至 AC（过程略），并用 **dir \*.zip** 命令查看上传完的文件。

```
<AC> dir *.zip
Directory of cfa0:/
0      -rw-      66127  Nov 27 2013 10:39:08   ssid1.zip
1020068 KB total (502420 KB free)
File system type of cfa0: FAT32
```

#### (6) 配置 SSID 绑定自定义页面文件

# 将 **SSID: service 1** 与页面文件 **ssid1.zip** 绑定。

```
<AC> system-view
[AC] portal local-server bind ssid service1 file ssid1.zip
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 **GigabitEthernet1/0/1** 接口的属性为 **trunk**，当前 trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 **GigabitEthernet1/0/2** 接口属性为 **access**，并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 使能 DHCP 服务。

```
[Switch] dhcp enable
```

# 创建名为 **vlan100** 的 DHCP 地址池，配置地址池范围为 **188.10.0.2~188.10.0.5**，网关地址为 **188.10.0.6**，为 AP 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan100 extended
```

```
[Switch-dhcp-pool-vlan100] network ip range 188.10.0.2 188.10.0.5
```

```
[Switch-dhcp-pool-vlan100] network mask 255.255.255.0
```

```
[Switch-dhcp-pool-vlan100] gateway-list 188.10.0.6
```

```
[Switch-dhcp-pool-vlan100] quit
```

# 创建名为 **vlan300** 的 DHCP 地址池，配置地址池范围为 **188.30.0.2~188.30.0.5**，网关地址为 **188.30.0.6**，为 Client 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan300 extended
```

```
[Switch-dhcp-pool-vlan300] network ip range 188.30.0.2 188.30.0.5
```

```
[Switch-dhcp-pool-vlan300] network mask 255.255.255.0
```

```
[Switch-dhcp-pool-vlan300] gateway-list 188.30.0.6
```

```
[Switch-dhcp-pool-vlan300] quit
```

### 3.4.3 RADIUS server 的配置



说明

下面以 iMC 为例(使用 iMC 版本为：iMC PLAT 7.0 (E0202)、iMC UAM 7.0 (E0202)，说明 RADIUS server 的基本配置。

---

#### # 增加接入设备

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，单击“增加”按钮，进入“增加接入设备”页面，单击<手工增加>按钮，进入“手工增加接入设备”页面。

- 填写起始 IP 地址为 **188.10.0.6**，该 IP 地址为 AC 上配置的 radius scheme 视图下的 nas-ip 地址。
- 单击<确定>按钮完成操作。
- 在“接入配置”页面配置共享密钥为 **123456**，该共享密钥与 AC 上配置 Radius 服务器时的密钥一致。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 帮助

接入配置

认证端口 \*

1812

计费端口 \*

1813

组网方式

不启用混合组网

业务类型

LAN接入业务

接入设备类型

H3C(General)

接入设备分组

无

共享密钥 \*

\*\*\*\*\*

确认共享密钥 \*

\*\*\*\*\*

业务分组

未分组

设备列表

选择

手工增加

全部清除

| 设备名称 | 设备IP地址     | 设备型号 | 备注 | 删除 |
|------|------------|------|----|----|
|      | 188.10.0.6 |      |    |    |

共有1条记录。

确定

取消

## # 配置接入策略

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，点击<增加>按钮，进入“增加接入策略”页面。

- 接入策略名填写 **portal**。该名称可以自行定义。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略 帮助

基本信息

接入策略名 \*

portal

业务分组 \*

未分组

描述

授权信息

接入时段

无

下行速率(Kbps)

优先级

证书认证

☒ 不启用 ☐ EAP证书认证 ☐ WAP证书认证

认证证书类型

EAP-TLS认证

下发VLAN

☐ 下发User Profile

☐ 下发ACL

分配IP地址 \*

否

上行速率(Kbps)

☐ 启用RSA认证

下发用户组

## # 配置接入服务

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，点击<增加>按钮，进入“增加接入服务”页面。

- 服务名填写 **portal**。该名称可以自行定义。
- 缺省接入策略选择 “portal”。即上一步配置的接入策略名。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

基本信息

服务名 \*

portal

业务分组 \*

未分组

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 (PC)

服务描述

☒可申请

☐Portal无感知认证

服务后缀

缺省接入策略 \*

portal

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

## # 配置接入用户

选择“用户”页签，单击导航树中的[增加用户]菜单项，进入“增加用户”页面。

- 用户姓名填写 **Test**。该名称可以自行定义。
- 证件号码填写 **123**。该名称可以自行定义。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 增加用户 帮助

增加用户

基本信息

用户姓名 \*

Test

证件号码 \*

123

通讯地址

电子邮件

电话

用户分组 \*

未分组

☐开通自助帐户

检查是否可用

确定

取消

添加用户完成后，会跳转到“增加用户结果页面”，单击[增加用户账号]进入“增加接入用户”视图。

用户 > 增加用户结果 帮助

增加用户完成，您可继续选择如下操作：

[增加用户账号](#)

[返回用户列表](#)

[查看用户详细信息](#)

[继续增加用户](#)

[增加接入用户帐号。](#)

[返回用户列表。](#)

[查看刚刚增加的用户的信息。](#)

[继续增加新的用户。](#)

在“增加接入用户”视图下。

- 账户名填写 **test**。该名称可以自行定义。
- 密码填写 **123456**。该名称可以自行定义。
- 接入服务选择上一步配置的接入服务“portal”。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 接入用户 > 增加接入用户 帮助

### 接入用户

#### 接入信息

用户姓名 \*  选择 增加用户  
 帐号名 \*   
☐ 预开用户 ☐ 缺省BYOD用户 ☐ 主机名用户 ☐ 快速认证用户  
 密码 \*  密码确认 \*   
☒ 允许用户修改密码 ☐ 启用用户密码控制策略 ☐ 下次登录须修改密码  
 生效时间  至  失效时间  至  
 最大闲置时长(分钟)  在线数量限制   
 Portal无感知认证最大绑定数   
 登录提示信息

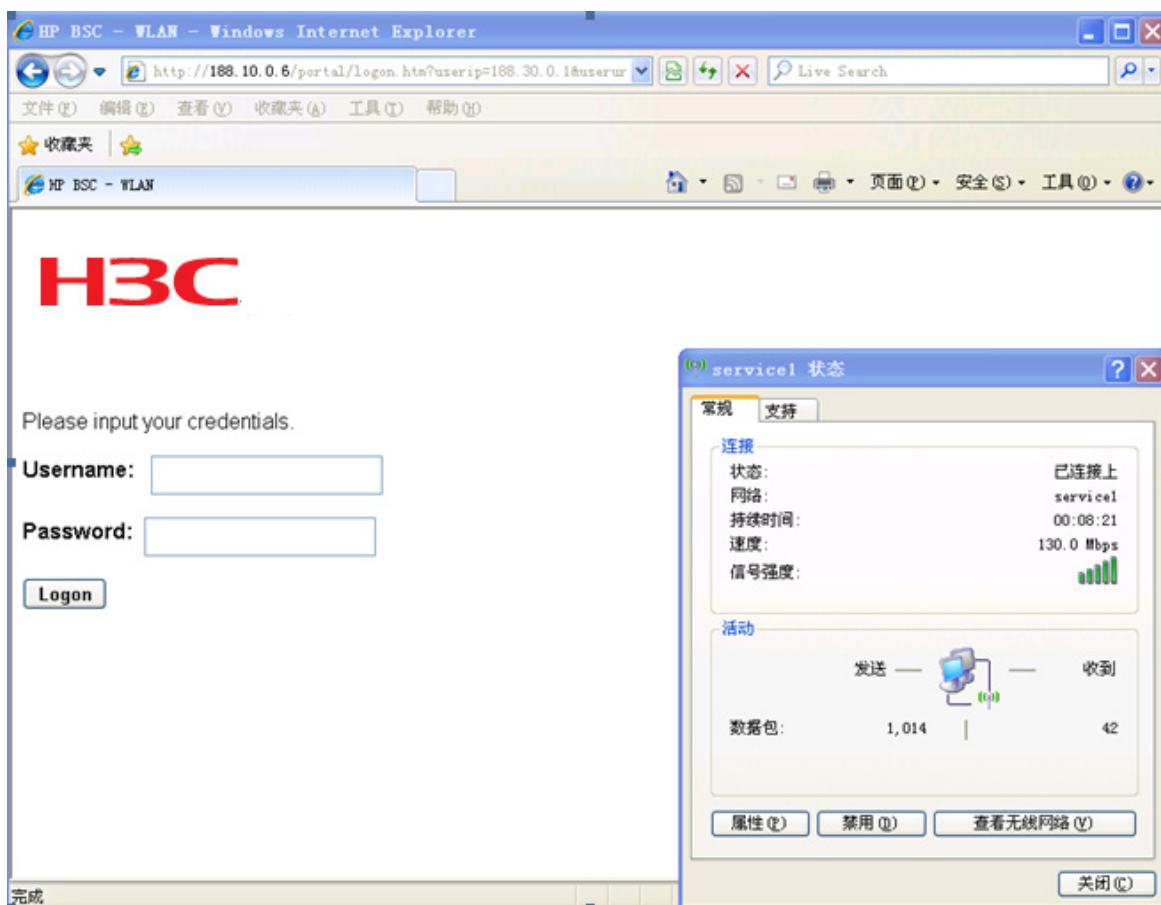
#### 接入服务

| 服务名                               | 服务后缀 | 状态  | 分配IP地址 |
|-----------------------------------|------|-----|--------|
| <input type="checkbox"/> lyportal |      | 可申请 |        |
| <input type="checkbox"/> mp       |      | 可申请 |        |
| ... portal                        |      | 可申请 |        |

## 3.5 验证配置

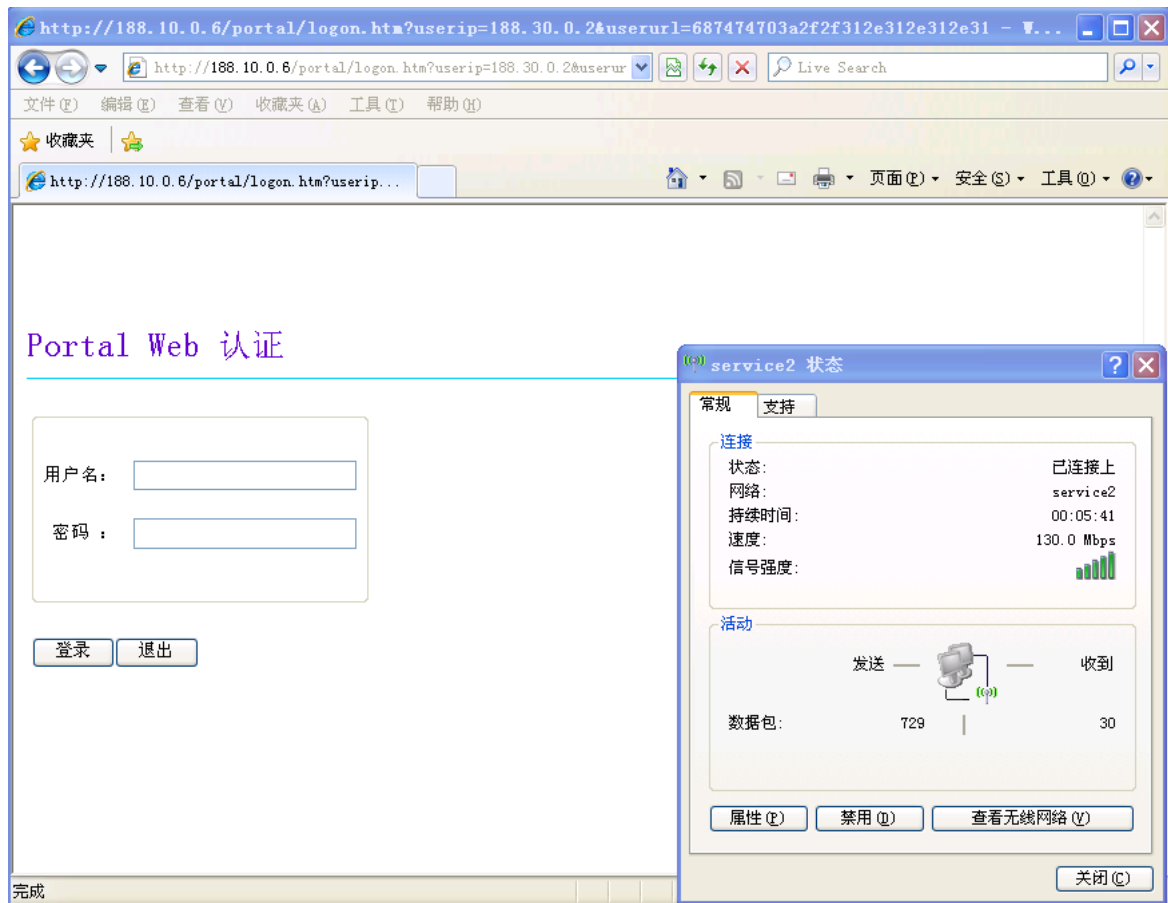
# Client 1 通过无线服务 service 1 上线后，进行 Portal 认证时，弹出自定义的认证页面。

图2 自定义认证页面



# Client 2 通过无线服务 service 2 上线后，由于没有配置其绑定的自定义认证页面，所以客户端进行 Portal 认证时推出的是系统默认认证页面。

图3 系统默认认证页面



## 3.6 配置文件

- AC:

```
#
radius nas-ip 188.10.0.6
#
portal server office ip 188.10.0.6
portal local-server http
portal local-server bind ssid service1 file ssid1.zip
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
primary authentication 8.1.1.5
key authentication cipher $c$3$lRA4cjtdvxqsRUuMR42kkQWa3b9Yw9Hk7A==
user-name-format without-domain
```

```

#
domain office
    authentication portal radius-scheme office
    authorization portal radius-scheme office
    accounting portal none
    access-limit disable
    state active
    idle-cut disable
    self-service-url disable
#
wlan service-template 1 clear
    ssid service1
    bind WLAN-ESS 1
    service-template enable
#
wlan service-template 2 clear
    ssid service2
    bind WLAN-ESS 2
    service-template enable
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200 300
#
interface Vlan-interface100
    ip address 188.10.0.6 255.255.0.0
#
interface Vlan-interface300
    ip address 188.30.0.6 255.255.0.0
    portal server office method direct
    portal domain office
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
interface WLAN-ESS2
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
    serial-id 21023529G007C000020

```

```

radio 1
radio 2
  service-template 1 vlan-id 300
  service-template 2 vlan-id 300
radio enable
#
•   Switch:
#
vlan 100
#
vlan 300
#
dhcp server ip-pool vlan100 extended
  network ip range 188.10.0.2 188.10.0.5
  network mask 255.255.255.0
  gateway-list 188.10.0.6
#
dhcp server ip-pool vlan300 extended
  network ip range 188.30.0.2 188.30.0.5
  network mask 255.255.255.0
  gateway-list 188.30.0.6
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 100 300
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
  poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。



# 本地转发+Portal 认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                               |    |
|-------------------------------|----|
| 1 简介.....                     | 1  |
| 2 配置前提 .....                  | 1  |
| 3 AC 为无线客户端集中分配地址方式配置举例 ..... | 1  |
| 3.1 组网需求 .....                | 1  |
| 3.2 配置思路 .....                | 2  |
| 3.3 配置注意事项.....               | 2  |
| 3.4 配置步骤 .....                | 2  |
| 3.4.1 配置 Switch A .....       | 2  |
| 3.4.2 配置 AC.....              | 3  |
| 3.4.3 配置 Router.....          | 6  |
| 3.4.4 配置 Switch B .....       | 6  |
| 3.4.5 apcfg.txt 配置文件 .....    | 7  |
| 3.4.6 配置 Portal server .....  | 7  |
| 3.5 验证配置 .....                | 14 |
| 3.6 配置文件 .....                | 16 |
| 4 分支机构独立为无线客户端分配地址配置举例.....   | 19 |
| 4.1 组网需求 .....                | 19 |
| 4.2 配置思路 .....                | 20 |
| 4.3 配置注意事项.....               | 20 |
| 4.4 配置步骤 .....                | 20 |
| 4.4.1 配置 Switch A .....       | 20 |
| 4.4.2 配置 AC.....              | 21 |
| 4.4.3 配置 Router.....          | 24 |
| 4.4.4 配置 Switch B .....       | 25 |
| 4.4.5 apcfg.txt 配置文件 .....    | 25 |
| 4.4.6 配置 Portal 服务器 .....     | 26 |
| 4.4.7 验证配置 .....              | 33 |
| 4.4.8 配置文件 .....              | 35 |
| 5 相关资料 .....                  | 38 |

# 1 简介

本文档介绍 WLAN 集中 portal 认证+本地转发的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 XXX 特性。

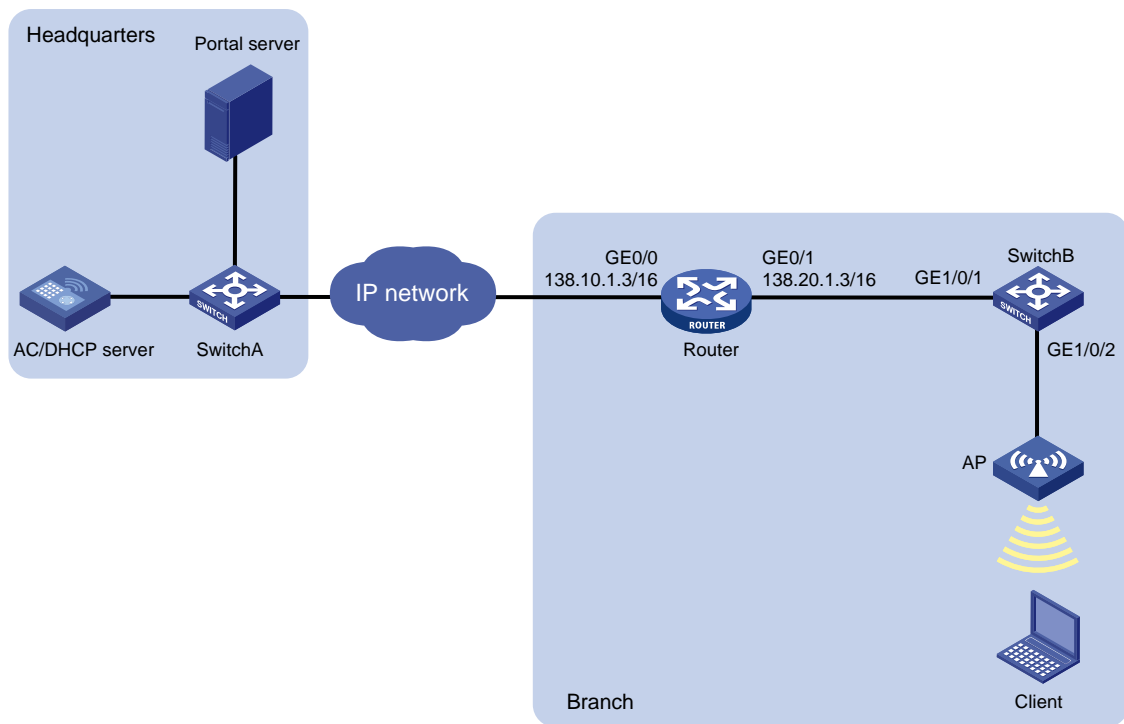
## 3 AC 为无线客户端集中分配地址方式配置举例

### 3.1 组网需求

如图 1 所示，总部的 AC 与分支机构的 AP 跨三层关联并作为 DHCP server 为 Client 分配 IP 地址；Router 作为 Client 的网关并为 AP 分配 IP 地址，具体要求如下：

- 用户通过 Portal 认证接入无线网络；
- 用户通过 Portal 认证后，AC 将用户规则下发到 AP 上，用户报文在 AP 上直接做转发。

图1 AC 为无线客户端集中分配地址方式配置举例组网图



## 3.2 配置思路

- 为实现 AC 与 Portal 服务器通信，需要在 Switch A 上配置到 Portal 服务器的静态路由；
- 在 AC 上配置 DHCP 功能，使 AC 统一分配、集中管理各分支机构中无线客户端的地址；
- 为了使 AP 能够直接转发 Client 报文，需要在 AC 的服务模板下开启本地转发功能，同时通过下发 map-configuration 文件来对 AP 进行配置实现本地转发。

## 3.3 配置注意事项

- 无线客户端的 DHCP 地址池中的网关要指向 Router；
- AC 上要配置从 WLAN 获取用户信息的功能；
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 配置 Switch A

# 创建 VLAN 10 及其对应的 VLAN 接口，并为该接口配置 IP 地址，用来和 AC 通信。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface vlan 10
[SwitchA-Vlan-interface10] ip address 138.10.1.1 16
[SwitchA-Vlan-interface10] quit
```

# 创建 VLAN 20 及其对应的 VLAN 接口，并为该接口配置 IP 地址，用来和 AP 通信。

```
[SwitchA] vlan 20
[SwitchA-vlan20] quit
[SwitchA] interface vlan 20
[SwitchA-Vlan-interface20] ip address 138.20.1.1 16
[SwitchA-Vlan-interface20] quit
```

# 创建 VLAN 30 及其对应的 VLAN 接口，并为该接口配置 IP 地址，用来和 Client 通信。

```
[SwitchA] vlan 30
[SwitchA-vlan30] quit
[SwitchA] interface vlan 30
[SwitchA-Vlan-interface30] ip address 138.30.1.1 16
[SwitchA-Vlan-interface30] quit
```

# 创建 VLAN 138 及其对应的 VLAN 接口，并为该接口配置 IP 地址，用来和 Portal 服务器通信。

```
[SwitchA] vlan 138
[SwitchA-vlan138] quit
[SwitchA] interface vlan 138
[SwitchA-Vlan-interface138] ip address 8.138.1.2 16
[SwitchA-Vlan-interface138] quit
```

# 创建聚合口 4。

```
[SwitchA] interface bridge-aggregation 4
```

```
[SwitchA-Bridge-Aggregation4] quit
# 配置 SwitchA 与 AC 连接的接口加入聚合口 4。
[SwitchA] interface ten-gigabitethernet 4/0/1
[SwitchA-Ten-GigabitEthernet4/0/1] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/1] quit
[SwitchA] interface ten-gigabitethernet 4/0/2
[SwitchA-Ten-GigabitEthernet4/0/2] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/2] quit
# 配置聚合口为 Trunk 口，并允许所有 VLAN 通过。
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port link-type trunk
[SwitchA-Bridge-Aggregation4] port trunk permit vlan all
[SwitchA-Bridge-Aggregation4] quit
# 配置静态路由，用于 AC 与 Portal 服务器通信，下一跳指向与 Portal 服务器互通的网关。
[SwitchA] ip route-static 8.0.0.0 8 8.138.1.1
```

### 3.4.2 配置 AC

#### (1) 配置 AC 接口

# 创建 VLAN 10 及其对应的 VLAN 接口，并为该接口配置 IP 地址，用来和 Portal 服务器通信。

```
<AC> system-view
[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 138.10.1.80 255.255.0.0
[AC-Vlan-interface10] quit
```

# 创建 VLAN 30 及其对应的 VLAN 接口，并为该接口配置 IP 地址，用来进行 Portal 认证。

```
[AC] vlan 30
[AC-vlan30] quit
[AC] interface vlan-interface 30
[AC-Vlan-interface30] ip address 138.30.1.80 255.255.0.0
[AC-Vlan-interface30] quit
```

# 创建聚合口 1。

```
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] quit
```

# 将 AC 上两个物理口加入聚合口 1。

```
[AC] interface ten-gigabitethernet 1/0/1
[AC-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
[AC-Ten-GigabitEthernet1/0/1] quit
[AC] interface ten-gigabitethernet 1/0/2
[AC-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
[AC-Ten-GigabitEthernet1/0/2] quit
```

# 配置 AC 聚合口 1 的类型为 Trunk 口并允许所有 VLAN 通过，用来和 AP、Client 通信。

```
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] port link-type trunk
[AC-Bridge-Aggregation1] port trunk permit vlan all
```

```
[AC-Bridge-Aggregation1] quit
```

## (2) 配置 DHCP 服务

# 使能 DHCP 功能。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 30，用于为 Client 动态分配地址，并将网关指向 Switch B。

```
[AC] dhcp server ip-pool 30
```

```
[AC-dhcp-pool-10] network 138.30.0.0 16
```

```
[AC-dhcp-pool-10] gateway-list 138.30.1.2
```

```
[AC-dhcp-pool-10] dns-list 138.20.1.3
```

```
[AC-dhcp-pool-10] dns-list 8.1.1.5
```

```
[AC-dhcp-pool-10] quit
```

## (3) 配置 WLAN-ESS 接口

# 创建接口 WLAN-ESS 30。

```
[AC] interface wlan-ess 30
```

# 配置端口的链路类型为 Access，允许 VLAN 30 通过。

```
[AC-WLAN-ESS30] port access vlan 30
```

```
[AC-WLAN-ESS30] quit
```

## (4) 配置无线服务模板

# 创建 clear 类型的无线服务模板 service1。

```
[AC] wlan service-template service1 clear
```

# 设置当前服务模板的 SSID 为 portal-local。

```
[AC-wlan-st-service1] ssid portal-local
```

# 将 WLAN-ESS30 接口绑定到无线服务模板 service1。

```
[AC-wlan-st-service1] bind wlan-ess 30
```

# 开启用户本地转发功能。

```
[AC-wlan-st-service1] client forwarding-mode local
```

# 开启无线客户端透传 DHCP 报文到 AC 的功能。

```
[AC-wlan-st-service1] client dhcp-server centralized
```

# 使能无线服务模板。

```
[AC-wlan-st-service1] service-template enable
```

```
[AC-wlan-st-service1] quit
```

## (5) 在 AC 下绑定无线服务模板

# 创建 AP 模板，名称为 ap1，型号名称选择 WA2620E-AGN，并配置其序列号。

```
[AC] wlan ap ap1 model WA2620E-AGN
```

```
[AC-wlan-ap-ap1] serial-id 210235A42MB108000002
```

```
[AC-wlan-ap-ap1] map-configuration apcfg.txt
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-ap1] radio 1
```

# 配置射频的工作信道为 161。

```
[AC-wlan-ap-ap1-radio-1] channel 161
```

# 将无线服务模板 service1 绑定到 AP 的 radio 1 口。

```
[AC-wlan-ap-ap1-radio-1] service-template service1
```

```
[AC-wlan-ap-ap1-radio-1] radio enable
```

```
[AC-wlan-ap-ap1-radio-1] quit
```

```
[AC-wlan-ap-ap1]quit
```

## (6) 配置 Portal 认证

# 配置 Portal 认证服务器地址为 8.1.1.50，并指定服务器对应的 URL。

```
[AC] portal server pt ip 8.1.1.50 key simple 123456 url http://8.1.1.50:8080/portal
```

# 配置 Portal 免认证规则 1，用来放行 AC 上配置 Portal 认证服务的接口能够与 Portal 服务器通信。

```
[AC] portal free-rule 1 source interface bridge-aggregation1 destination any
```

# 配置 AC 通过 WLAN 获取 Portal 用户信息。

```
[AC] portal host-check wlan
```

# 配置 RADIUS 方案 portal。

```
[AC] radius scheme portal
```

# 配置认证、计费 and 授权服务器的 IP 地址为 8.1.1.50。

```
[AC-radius-portal] primary authentication 8.1.1.50
```

```
[AC-radius-portal] primary accounting 8.1.1.50
```

# 配置与认证、计费 and 授权服务器交互报文时的共享密钥为 123456。

```
[AC-radius-portal] key authentication simple 123456
```

```
[AC-radius-portal] key accounting simple 123456
```

# 指定发送给 RADIUS 服务器的用户名不携带域名。

```
[AC-radius-portal] user-name-format without-domain
```

# 配置设备发送 RADIUS 报文使用的源 IP 地址为 138.10.1.80。

```
[AC-radius-portal] nas-ip 138.10.1.80
```

```
[AC-radius-portal] quit
```

# 配置 AAA 认证域 portal。

```
[AC] domain portal
```

# 设置 ISP 域的认证、授权和计费方法均为 RADIUS。

```
[AC-isp-portal] authentication portal radius-scheme portal
```

```
[AC-isp-portal] accounting portal radius-scheme portal
```

```
[AC-isp-portal] authorization portal radius-scheme portal
```

```
[AC-isp-portal] quit
```

# 配置接口 VLAN 30 为 Portal 直接认证的接口。

```
[AC] interface vlan-interface 30
```

```
[AC-Vlan-interface30] portal server pt method direct
```

# 指定从接口接入的 IPv4 Portal 用户使用认证域为 portal。

```
[AC-Vlan-interface30] portal domain portal
```

# 配置接口发送 Portal 报文使用的 IPv4 源地址为 138.10.1.80。

```
[AC-Vlan-interface30] portal nas-ip 138.10.1.80
```

# 开启 Portal 本地转发功能。

```
[AC-Vlan-interface30] portal forwarding-mode local
```

```
[AC-Vlan-interface30] quit
```

# 配置 AC 与 AP 和 Portal 服务器通信的静态路由下一跳为 Switch A 的接口 VLAN 10。

```
[AC] ip route-static 0.0.0.0 0 138.10.1.1
```

# 开启 arp-snooping 功能。

```
[AC] arp-snooping enable
```

# 开启 learn-ipaddr 功能

```
[AC] wlan client learn-ipaddr enable
```

### 3.4.3 配置 Router

# 配置 GigabitEthernet0/0 的 IP 地址，用来和 AC 通信。

```
<Router> system-view
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] ip address 138.10.1.3 255.255.0.0
[Router-GigabitEthernet0/0] quit
```

# 配置 GigabitEthernet0/1 的 IP 地址。

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] ip address 138.20.1.3 255.255.0.0
[Router-GigabitEthernet0/1] quit
```

# 使能 DHCP 功能。

```
[Router] dhcp enable
```

# 配置 DHCP 地址池 20，用于为 AP 动态分配地址，并通过 option43 指定关联的 AC。

```
[Router] dhcp server ip-pool 20
[Router-dhcp-pool-20] network 138.20.0.0 255.255.0.0
[Router-dhcp-pool-20] gateway-list 138.20.1.3
[Router-dhcp-pool-20] option 43 hex 80070000 018A0A01 50
[Router-dhcp-pool-20] quit
```

# 配置 Router 到公网的静态路由，下一跳指向 AC 交换侧的地址。

```
[Router] ip route-static 0.0.0.0 0 138.10.1.1
```

### 3.4.4 配置 Switch B

# 创建 VLAN 20，并配置对应接口 IP 地址，用来和 Router 通信。

```
<SwitchB> system-view
[SwitchB] vlan 20
[SwitchB-vlan20] quit
[SwitchB] interface vlan-interface 20
[SwitchB-Vlan-interface20] ip address 138.20.1.2 255.255.0.0
[SwitchB-Vlan-interface20] quit
```

# 配置 GigabitEthernet1/0/1 的类型为 Trunk，允许所有 VLAN 通过。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/1] quit
```

# 配置 GigabitEthernet1/0/2 接口属性，使能 PoE 为 AP 供电，类型为 Trunk，允许所有 VLAN 通过，且 PVID 设置为 20。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] poe enable
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/2] port trunk pvid vlan 20
[SwitchB-GigabitEthernet1/0/2] quit
```

# 创建 VLAN 30，并配置对应接口的 IP 地址，用来和无线客户端通信。

```
[SwitchB] vlan 30
```



```
[SwitchB-vlan30] quit
[SwitchB] interface vlan-interface 30
[SwitchB-Vlan-interface30] ip address 138.30.1.2 255.255.0.0
[SwitchB-Vlan-interface30] quit
# 配置与公网设备通信的静态路由，下一跳指向与 Router 直连的接口。
[SwitchB] ip route-static 0.0.0.0 0 138.20.1.3
```

### 3.4.5 apcfg.txt 配置文件

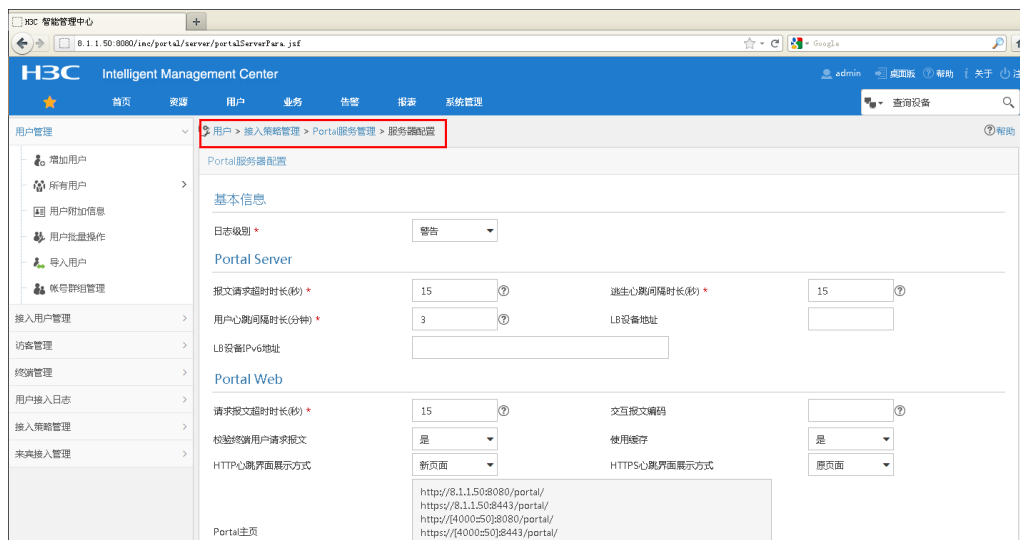
```
# 配置 Portal 服务器地址为 8.1.1.50，并指定服务器对应的 url。
system-view
portal server pt ip 8.1.1.50 key simple 123456 url http://8.1.1.50:8080/portal
# 配置 Portal 免认证规则 1，用来放行 AP 上开启 Portal 认证服务的接口能够与 Portal 服务器通信。
portal free-rule 1 source interface GigabitEthernet 1/0/1 destination any
# 配置移动需求的 Portal 参数。
portal device-id beijing-ac-01
portal url-param include nas-id param-name vlan
portal url-param include user-mac des-encrypt param-name wlanusermac
portal url-param include nas-ip param-name wlanacip
portal url-param include ap-mac param-name wlanapmac
portal url-param include user-url param-name wlanfirsturl
portal url-param include user-ip param-name wlanuserip
portal url-param include ac-name param-name wlanacname
portal url-param include ssid
portal host-check wlan
# 创建 vlan 30。
vlan 30
# 创建 VLAN 30 对应接口，并进入接口 VLAN 30 视图
interface vlan 30
# 接口下指定 Portal 服务器并配置为直接认证方式。
portal server pt method direct
# 配置接口发送 Portal 报文使用的源地址为 AC 的地址。
portal nas-ip 138.10.1.80
# 进入到 AP 的物理接口 GigabitEthernet1/0/1。
interface GigabitEthernet 1/0/1
# 配置接口 GigabitEthernet1/0/1 类型为 Trunk。
port link-type trunk
# 配置接口 GigabitEthernet1/0/1 允许所有 VLAN 通过。
port trunk permit vlan all
```

### 3.4.6 配置 Portal server

- (1) 配置 Portal 服务
- # 配置 Portal 服务器。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，使用缺省配置。

图2 Portal 服务器配置页面

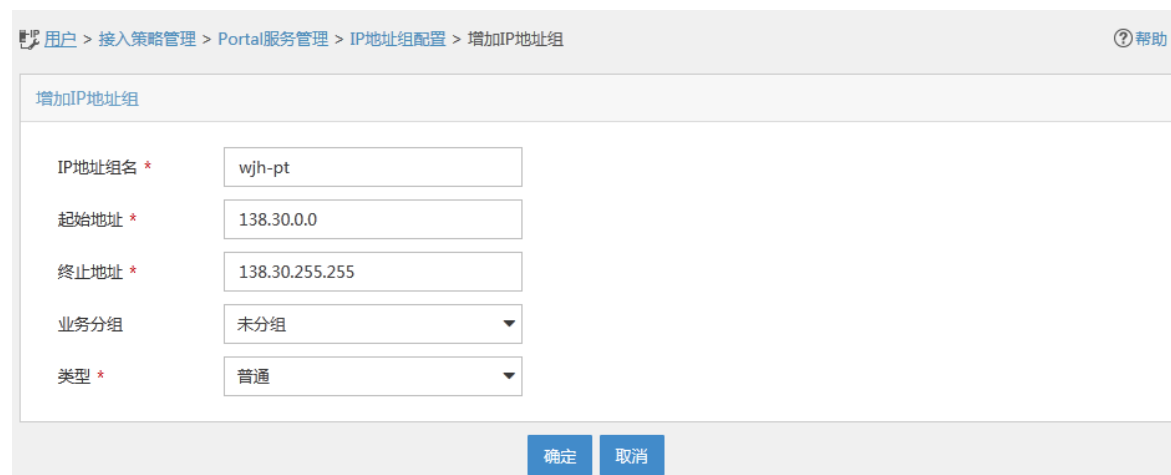


#### # 配置 IP 地址组。

选择“用户”页签，单击导航树[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入 IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 输入 IP 地址组名：wjh-pt;
- 输入起始地址：138.30.0.0;
- 输入终止地址：138.30.255.255;
- 其他采用缺省配置，单击<确定>按钮完成操作。

图3 增加 IP 地址组配置页面



#### # 增加 Portal 设备。

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入设备配置页面。在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 输入设备名：wjh;

- 输入 IP 地址：即 AC 上配置的 portal bas-ip 地址，138.10.1.80；
- 输入密钥：123456，与 AC 上配置的 Portal server 密钥一致；
- 其他采用默认配置，单击<确定>按钮完成操作。

图4 增加设备信息配置页面



图4展示了“增加设备信息”配置页面。页面顶部有面包屑导航：用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息。右侧有“帮助”链接。页面主体包含以下配置项：

|          |            |               |             |
|----------|------------|---------------|-------------|
| 设备名 *    | wjh        | 业务分组 *        | 未分组         |
| 版本 *     | Portal 2.0 | IP地址 *        | 138.10.1.80 |
| 监听端口 *   | 2000       | 本地Challenge * | 否           |
| 认证重发次数 * | 0          | 下线重发次数 *      | 1           |
| 支持逃生心跳 * | 否          | 支持用户心跳 *      | 否           |
| 密钥 *     | •••••      | 确认密钥 *        | •••••       |
| 组网方式 *   | 三层         |               |             |
| 设备描述     |            |               |             |

底部有“确定”和“取消”按钮。

# 增加端口组信息。


在 Portal 设备配置页面中的设备信息列表中，单击<端口组信息管理>按钮（“”图标），进入端口组信息配置页面。

图5 设备配置页面



图5展示了“设备配置”页面。页面顶部有面包屑导航：用户 > 接入策略管理 > Portal服务管理 > 设备配置。右侧有“加入收藏”和“帮助”链接。页面主体包含以下部分：

**设备信息查询**

|      |  |      |  |
|------|--|------|--|
| 设备名  |  | 版本   |  |
| 下发结果 |  | 业务分组 |  |

右侧有“查询”和“重置”按钮。

**增加**

| 设备名 | 版本         | 业务分组 | IP地址        | 最近一次下发时间 | 下发结果 | 操作                                                                                                                                                                                                                                                                                                                                                      |
|-----|------------|------|-------------|----------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wjh | Portal 2.0 | 未分组  | 138.10.1.80 |          | 未下发  |     |

底部显示：共有1条记录，当前第1 - 1，第 1/1 页。右侧有分页控件，显示“1”和“50”。

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 输入端口组名：w-group；
- 选择 IP 地址组：wjh-pt；

- 其他采用默认配置，单击<确定>按钮完成操作。

图6 增加端口组信息

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 增加端口组信息 帮助

增加端口组信息

|            |         |            |        |
|------------|---------|------------|--------|
| 端口组名 *     | w-group | 提示语言 *     | 动态检测   |
| 开始端口 *     | 0       | 终止端口 *     | zzzzzz |
| 协议类型 *     | HTTP    | 快速认证 *     | 否      |
| 是否NAT *    | 否       | 错误透传 *     | 是      |
| 认证方式 *     | CHAP认证  | IP地址组 *    | wjh-pt |
| 心跳间隔(分钟) * | 10      | 心跳超时(分钟) * | 30     |
| 用户域名       |         | 端口组描述      |        |
| 无感知认证      | 不支持     | 客户端防破解 *   | 否      |
| 页面推送策略     |         | 缺省认证页面     |        |

确定 取消

(2) 配置接入服务

# 增加接入设备

选择“用户”标签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面。在该页面中单击<增加>按钮，进入增加接入设备页面。

选择手工增加接入设备，添加 IP 地址为 138.10.1.80 的接入设备，与 AC 上 RADIUS 方案中的 nas-ip 一致；

图7 手工增加接入设备

手工增加接入设备

|          |             |
|----------|-------------|
| 起始IP地址 * | 138.10.1.80 |
| 结束IP地址   |             |
| 备注       |             |

确定 取消

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”，该密码与 AC 配置 RADIUS 方案时的地址一致；
- 选择接入设备类型为“H3C(General)”；

- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \*

1812

计费端口 \*

1813

组网方式

不启用混合组网

业务类型

LAN接入业务

接入设备类型

H3C(General)

业务分组

未分组

共享密钥 \*

.....

确认共享密钥 \*

.....

接入设备分组

无

设备列表

选择

手工增加

全部清除

| 设备名称 | 设备IP地址      | 设备型号 | 备注 | 删除 |
|------|-------------|------|----|----|
|      | 138.10.1.80 |      |    |    |

共有1条记录。

确定

取消

# 增加接入策略。

选择“用户”标签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略配置页面。  
在接入策略列表中单击<增加>按钮，进入增加接入策略页面。

- 接入策略名输入“wjh-portal”；
- 业务分组“未分组”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

帮助

基本信息

接入策略名 \*

wjh-portal

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☒ 不启用 ☐ EAP证书认证 ☐ WAPI证书认证

认证证书类型

EAP-TLS认证

下发VLAN

下发用户组

☐ 下发User Profile

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Windows可溶解客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔(分钟) 30

自动重连次数 3

客户端最低版本 1.00-0120

违规处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式 ☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定

取消

# 增加接入服务。

选择“用户”标签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务配置页面。在接入服务列表中点击<增加>按钮。

- 服务名输入“wjh-portal”；
- 缺省接入策略“wjh-portal”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图10 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

|                                         |                                      |               |            |
|-----------------------------------------|--------------------------------------|---------------|------------|
| 服务名 *                                   | wjh-portal                           | 服务后缀          |            |
| 业务分组 *                                  | 未分组                                  | 缺省接入策略 *      | wjh-portal |
| 缺省私有属性下发策略 *                            | 不使用                                  | 缺省单帐号在线数量限制 * | 0          |
| 缺省单帐号最大绑定终端数 *                          | 0                                    |               |            |
| 服务描述                                    |                                      |               |            |
| <input checked="" type="checkbox"/> 可申请 | <input type="checkbox"/> Portal无感知认证 |               |            |

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | 优先级 | 修改 | 删除 |
|-------------|------|----------|-----|----|----|
| 未找到符合条件的记录。 |      |          |     |    |    |

确定 取消

(3) 增加接入用户。

# 选择“用户”标签，单击导航树中的[接入用户管理/接入用户]菜单项，进入到接入用户配置页面。在接入用户列表中点击<增加>按钮，进入增加接入用户页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“wjh-portal”；
- 输入证件号码“111111”；
- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图11 增加用户

增加用户

基本信息

|        |            |        |        |        |
|--------|------------|--------|--------|--------|
| 用户姓名 * | wjh-portal | 证件号码 * | 111111 | 检查是否可用 |
| 通讯地址   |            | 电话     |        |        |
| 电子邮件   |            | 用户分组 * | 未分组    |        |

确定 取消

- 账号名输入“wjh-portal”；
- 勾选接入服务“wjh-portal”；

- 单击<确定>按钮完成操作。

图12 增加接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

wjh-portal

选择

增加用户

帐号名 \*

wjh-portal

☐ 预开户用户

☐ 缺省BYOD用户

☐ MAC地址认证用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                            | 服务后缀 | 状态  | 分配IP地址 |
|------------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> wjh-portal |      | 可申请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线SSID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

IP地址

MAC地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

### 3.5 验证配置

# 无线客户端使用 SSID 为 portal-local 的无线服务模板上线，获取到地址。在浏览器中输入 Portal 服务器网段的任一地址，弹出 Portal 认证页面，输入 Portal 服务器上设置的用户名和密码进行认证上线。



图13 用户上线



# 当 Portal 用户认证成功并上线之后，AC 会将用户规则下发到 AP 设备上，用户报文在 AP 上直接做转发。在 AC 上通过命令 **display portal user interface** 查看成功上线的用户。

```
<AC> display portal user interface vlan 30
Index:0
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC                IP                Vlan  Interface
-----
0021-631e-7911    138.30.0.1        30    Vlan-interface10
On interface Vlan-interface10:total 1 user(s) matched, 1 listed.
```

# 在 AP 上通过命令 **display portal acl dynamic interface** 查看用户规则成功下发。

```
<ap1> display portal acl dynamic interface vlan-interface 30
IPv4 portal ACL rules on Vlan-interface10:
Rule 0
Inbound interface : all
Type               : dynamic
Action             : permit
Source:
  IP               : 138.30.0.1
  Mask             : 255.255.255.255
  MAC              : 0021-631e-7911
  Interface        : any
  VLAN             : 30
  Protocol         : 0
Destination:
  IP               : 0.0.0.0
  Mask             : 0.0.0.0
Author ACL:
  Number          : NONE
```

## 3.6 配置文件

- SwitchA

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 138
#
interface Bridge-Aggregation4
    port link-type trunk
    port trunk permit vlan all
#
interface Vlan-interface10
    ip address 138.10.1.1 255.255.0.0
#
interface Vlan-interface20
    ip address 138.20.1.1 255.255.0.0
#
interface Vlan-interface30
    ip address 138.30.1.1 255.255.0.0
#
interface Vlan-interface138
    ip address 8.138.1.2 255.255.0.0
#
interface Ten-GigabitEthernet4/0/1
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan all
    port link-aggregation group 4
#
interface Ten-GigabitEthernet4/0/2
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan all
    port link-aggregation group 4
#
ip route-static 8.0.0.0 255.0.0.0 8.138.1.1
#
```

- AC

```
#
portal server pt ip 8.1.1.50 key simple 123456 url http://8.1.1.50:8080/portal
portal free-rule 1 source interface Bridge-Aggregation1 destination any
portal host-check wlan
#
```

```

wlan client learn-ipaddr enable
#
vlan 10
#
vlan 30
#
dhcp server ip-pool 30
network 138.30.0.0 mask 255.255.0.0
gateway-list 138.30.1.2
dns-list 138.20.1.3
dns-list 8.1.1.5
#
radius scheme portal
primary authentication 8.1.1.50
primary accounting 8.1.1.50
key authentication simple 123456
key accounting simple 123456
user-name-format without-domain
nas-ip 138.10.1.80
#
domain portal
authentication portal radius-scheme portal
authorization portal radius-scheme portal
accounting portal radius-scheme portal
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template servicel clear
ssid portal-local
bind WLAN-ESS 30
client forwarding-mode local
client dhcp-server centralized
service-template enable
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan all
#
interface Vlan-interface10
ip address 138.10.1.80 255.255.0.0
#
interface Vlan-interface30
ip address 138.30.1.80 255.255.0.0
portal server pt method direct
portal domain portal
portal nas-ip 138.10.1.80

```

```

portal forwarding-mode local
#
interface Ten-GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan all
port link-aggregation group 1
#
interface WLAN-ESS30
port access vlan 30
#
wlan ap ap1 model WA2620E-AGN id 1
serial-id 210235A42MB108000002
map-configuration apcfg.txt
radio 1
channel 161
service-template service1
radio enable
radio 2
#
ip route-static 0.0.0.0 0.0.0.0 138.10.1.1
#
arp-snooping enable
#
dhcp enable
#
● Router
#
dhcp server ip-pool 20
network 138.20.0.0 mask 255.255.0.0
option 43 hex 80070000 018A0A01 50
#
interface GigabitEthernet0/0
port link-mode route
ip address 138.10.1.3 255.255.0.0
#
interface GigabitEthernet0/1
port link-mode route
ip address 138.20.1.3 255.255.0.0
#
ip route-static 0.0.0.0 255.0.0.0 138.10.1.1
#
dhcp enable
#

```

- SwitchB

```
#
vlan 20
#
vlan 30
#
interface Vlan-interface20
 ip address 138.20.1.2 255.255.0.0
#
interface Vlan-interface30
 ip address 138.30.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 description routeg0/1
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/2
 description ap-portal-local
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 20
 poe enable
#
 ip route-static 0.0.0.0 0.0.0.0 138.20.1.3
#
```

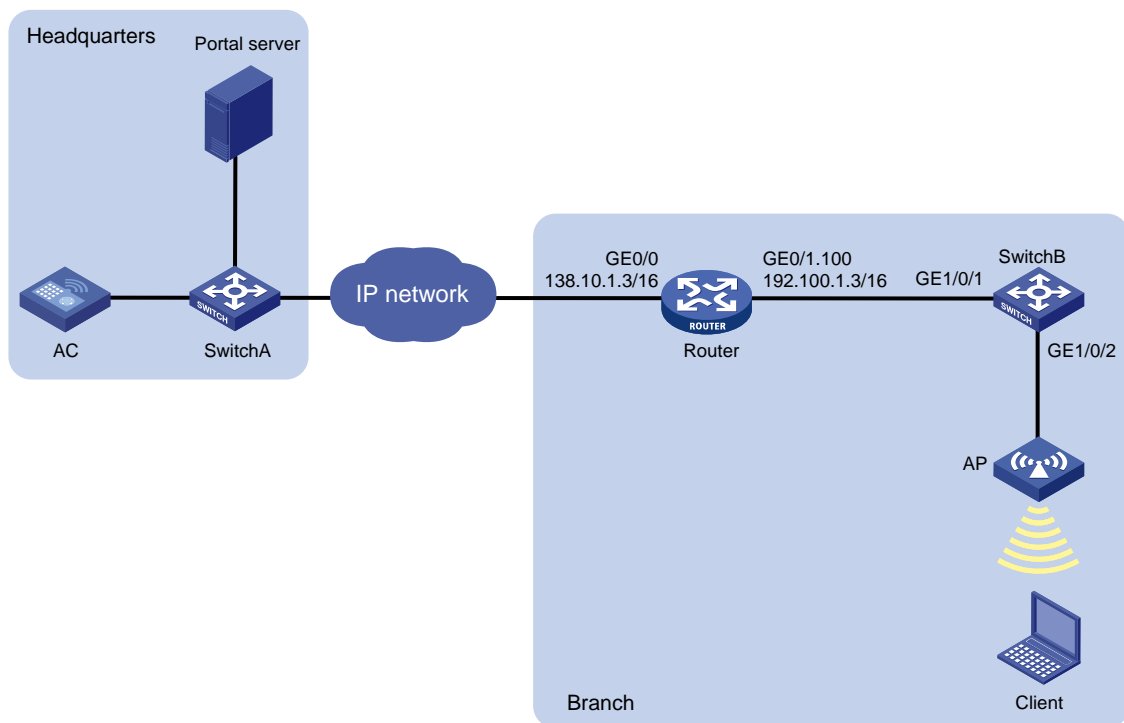
## 4 分支机构独立为无线客户端分配地址配置举例

### 4.1 组网需求

如 4.1 图 14 所示，总部的 AC 与分支机构的 AP 跨三层关联；Router 作为无线客户端的网关并为 AP 分配地址，具体要求如下：

- 用户通过 Portal 认证接入无线网络；
- 用户通过 Portal 认证后，AC 将用户规则下发到 AP 上，用户报文在 AP 上直接做转发。
- 各分支机构无线客户端的地址由各分支机构单独分配。

图14 分支机构独立分配无线客户端地址的组网图



## 4.2 配置思路

- 为实现 AC 与 Portal 服务器通信，Switch A 上配置 AC 与 Portal 服务器通信的静态路由。
- 为避免各分支机构中的无线客户端地址重复，Router 上配置为无线客户端分配地址的地址池。
- 为实现 Portal 集中认证，在 AC 和 AP 上配置 Portal 认证。
- 为了使 AP 能够直接转发 Client 报文，需要在 AC 的无线服务模板上开启本地转发功能，同时通过下发 map-configuration 文件来对 AP 进行配置实现本地转发。

## 4.3 配置注意事项

- AC 上要配置用户信息从 WLAN 获取的功能。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 4.4 配置步骤

### 4.4.1 配置 Switch A

# 创建 VLAN 10 及其对应的 VLAN 接口，并为该接口配置 IP 地址用来和 AC 通信。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface vlan 10
```

```
[SwitchA-Vlan-interface10] ip address 138.10.1.1 16
[SwitchA-Vlan-interface10] quit
# 创建 VLAN 138 及其对应的 VLAN 接口，并为该接口配置 IP 地址用来和 Portal 服务器通信。
[SwitchA] vlan 138
[SwitchA-vlan138] quit
[SwitchA] interface vlan 138
[SwitchA-Vlan-interface138] ip address 8.138.1.2 16
[SwitchA-Vlan-interface138] quit
# 创建聚合口 4。
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] quit
# 配置 SwitchA 与 AC 连接的接口加入聚合口。
[SwitchA] interface ten-gigabitethernet 4/0/1
[SwitchA-Ten-GigabitEthernet4/0/1] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/1] quit
[SwitchA] interface ten-gigabitethernet 4/0/2
[SwitchA-Ten-GigabitEthernet4/0/2] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/2] quit
# 配置聚合口为 Trunk 口，并允许所有 VLAN 通过。
[SwitchA] int bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port link-type trunk
[SwitchA-Bridge-Aggregation4] port trunk permit vlan all
[SwitchA-Bridge-Aggregation4] quit
# 配置静态路由，用于 Portal 服务器与 AC 之间通信，下一跳指向和 Portal 服务器互通的网关。
[SwitchA] ip route-static 8.0.0.0 8 8.138.1.1
```

## 4.4.2 配置 AC

### (1) 配置 AC 接口

# 创建 VLAN 10 及其对应的 VLAN 接口，并为该接口配置 IP 地址用来和 Portal 服务器通信。

```
<AC> system-view
[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 138.10.1.80 255.255.0.0
[AC-Vlan-interface10] quit
```

# 创建 VLAN 168 及其对应的 VLAN 接口，并为该接口配置 IP 地址用来配置 Portal 服务。

```
[AC] vlan 168
[AC-vlan168] quit
[AC] interface vlan-interface 168
[AC-Vlan-interface168] ip address 192.168.1.1 255.255.0.0
[AC-Vlan-interface168] quit
```

# 创建聚合口 1。

```
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] quit
```

# 将 AC 上两个物理口加入聚合口 1。

```

[AC] interface ten-gigabitethernet 1/0/1
[AC-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
[AC-Ten-GigabitEthernet1/0/1] quit
[AC] interface ten-gigabitethernet 1/0/2
[AC-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
[AC-Ten-GigabitEthernet1/0/2] quit
# 配置 AC 聚合口 1 的类型为 Trunk 口并允许所有 VLAN 通过。
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] port link-type trunk
[AC-Bridge-Aggregation1] port trunk permit vlan all
[AC-Bridge-Aggregation1] quit
(2) 配置 WLAN-ESS 接口
# 创建接口 WLAN-ESS 1。
[AC] interface wlan-ess 1
# 配置端口的链路类型为 Access，允许 VLAN 168 通过。
[AC-WLAN-ESS1] port access vlan 168
[AC-WLAN-ESS1] quit
(3) 配置无线服务模板
# 创建 clear 类型的服务模板 service1。
[AC] wlan service-template service1 clear
# 设置无线服务模板的 SSID 为 portal-local。
[AC-wlan-st-service1] ssid portal-local
# 将 WLAN-ESS 1 接口绑定到无线服务模板。
[AC-wlan-st-service1] bind wlan-ess 1
# 开启用户本地转发功能。
[AC-wlan-st-service1] client forwarding-mode local
# 使能无线服务模板。
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
(4) 在 AC 下绑定无线服务模板
# 创建 AP 模板，名称为 ap1，型号名称选择 WA2620E-AGN，并配置其序列号。
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 210235A42MB108000001
[AC-wlan-ap-ap1] map-configuration apcfg.txt
# 进入 radio 1 射频视图。
[AC-wlan-ap-ap1] radio 1
# 配置射频的工作信道为 161。
[AC-wlan-ap-ap1-radio-1] channel 161
# 将服务模板 service1 绑定到 AP 的 radio 1 口。
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
(5) 配置 Portal 认证

```



```

# 配置 Portal 服务器地址为 8.1.1.50，并指定服务器对应的 url。
[AC] portal server pt ip 8.1.1.50 key simple 123456 url http://8.1.1.50:8080/portal
# 配置 Portal 免认证规则 1，用于放行 AC 上起 Portal 的接口能够与 Portal 服务器通信。
[AC] portal free-rule 1 source interface Bridge-Aggregation1 destination any
# 配置 AC 通过 WLAN 来获取 Portal 用户的相关信息。
[AC] portal host-check wlan
# 配置 RADIUS 方案 portal。
[AC] radius scheme portal
# 配置认证、计费 and 授权服务器的 IP 地址为 8.1.1.50。
[AC-radius-portal] primary authentication 8.1.1.50
[AC-radius-portal] primary accounting 8.1.1.50
# 配置与认证、计费 and 授权服务器交互报文时的共享密钥均为 123456。
[AC-radius-portal] key authentication simple 123456
[AC-radius-portal] key accounting simple 123456
# 指定发送给 RADIUS 方案 portal 中 RADIUS 服务器的用户名不携带域名。
[AC-radius-portal] user-name-format without-domain
# 配置设备发送 RADIUS 报文使用的源 IP 地址为 138.10.1.80。
[AC-radius-portal] nas-ip 138.10.1.80
[AC-radius-portal] quit
# 配置 AAA 认证域 portal。
[AC] domain portal
# 设置 ISP 域的认证、授权和计费方法均为 RADIUS 方式。
[AC-isp-portal] authentication portal radius-scheme portal
[AC-isp-portal] accounting portal radius-scheme portal
[AC-isp-portal] authorization portal radius-scheme portal
[AC-isp-portal] quit
# 在接口 VLAN 168 上开启 Portal 直接认证。
[AC] interface vlan-interface 168
[AC-Vlan-interface168] portal server pt method direct
# 指定从接口接入的 IPv4 Portal 用户使用认证域为 portal。
[AC-Vlan-interface168] portal domain portal
# 配置接口发送 Portal 报文使用的 IPv4 源地址为 138.10.1.80。
[AC-Vlan-interface168] portal nas-ip 138.10.1.80
# 开启 Portal 本地转发功能。
[AC-Vlan-interface168] portal forwarding-mode local
[AC-Vlan-interface168] quit
# 配置与 Portal 服务器等公网设备通信的静态路由。
[AC] ip route-static 0.0.0.0 0 138.10.1.1
# 配置 arp-snooping 功能。
[AC] arp-snooping enable
# 配置 learn-ipaddr。
[AC] wlan client learn-ipaddr enable

```

### 4.4.3 配置 Router

# 配置接口 GigabitEthernet 0/0 的 IP 地址，用来与 AC 通信。

```
<Router> system-view
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] ip address 138.10.1.3 255.255.0.0
[Router-GigabitEthernet0/0] quit
```

# 创建子接口 GigabitEthernet 0/1.100，并配置 IP 地址，划分 VLAN 为 100，用来与 AP 通信。

```
[Router] interface gigabitethernet 0/1.100
[Router-GigabitEthernet0/1.100] ip address 192.100.1.3 255.255.0.0
[Router-GigabitEthernet0/1.100] vlan-type dot1q vid 100
[Router-GigabitEthernet0/1.100] quit
```

# 创建子接口 GigabitEthernet 0/1.168，并配置 IP 地址，划分 VLAN 为 168，用来与无线客户端通信。

```
[Router] interface gigabitethernet 0/1.168
[Router-GigabitEthernet0/1.168] ip address 192.168.2.3 255.255.255.0
[Router-GigabitEthernet0/1.168] vlan-type dot1q vid 168
[Router-GigabitEthernet0/1.168] quit
```

# 使能 DHCP 服务。

```
[Router] dhcp enable
```

# 配置 DHCP 地址池 100，用来为 AP 分配 IP 地址，并通过 option43 指定 AC 的地址。

```
[Router] dhcp server ip-pool 100
[Router-dhcp-pool-100] network 192.100.0.0 mask 255.255.0.0
[Router-dhcp-pool-100] gateway-list 192.100.1.3
[Router-dhcp-pool-100] option 43 hex 80070000 01 8a0a0150
[Router-dhcp-pool-100] quit
```

# 配置 DHCP 地址池 168，用于为无线客户端分配 IP 地址。

```
[Router] dhcp server ip-pool 168
[Router-dhcp-pool-168] network 192.168.2.0 mask 255.255.255.0
[Router-dhcp-pool-168] gateway-list 192.168.2.3
[Router-dhcp-pool-168] dns-list 192.168.2.3
[Router-dhcp-pool-168] dns-list 8.1.1.5
[Router-dhcp-pool-168] quit
```

# 创建 NAT 转换地址组 1，并指定转换后的地址为 NAT 网关出接口地址。

```
[NAT] nat address-group 1 138.10.1.3 138.10.1.3
```

# 创建 ACL 规则，用于触发 AP 和无线客户端进行 NAT 地址转换。

```
[NAT] acl number 3000
[NAT-acl-adv-3000] rule 1 permit ip source 192.100.0.0 0.0.255.255
[NAT-acl-adv-3000] rule 2 permit ip source 192.168.0.0 0.0.255.255
[NAT-acl-adv-3000] quit
```

# 在出接口上配置出方向动态地址转换，允许使用地址组 1 中的地址对内网访问外网的报文进行源地址转换。

```
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] nat outbound 3000 address-group 1
```

# 在出接口上使能 IP 虚拟分片重组功能，用来解决 NAT 地址转换时因报文太大导致转换失败的问题。

```
[Router-GigabitEthernet0/0] ip virtual-reassembly
[Router-GigabitEthernet0/0] quit
# 配置 Router 到 Portal 服务器的静态路由，下一跳指向 AC 交换侧的地址。
[Router] ip route-static 8.0.0.0 8 138.10.1.1
```

#### 4.4.4 配置 Switch B

```
# 创建 VLAN 100，并配置对应接口 IP 地址，用来和 Router 通信。
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 192.100.1.2 16
[SwitchB-Vlan-interface100] quit
# 配置接口 GigabitEthernet 1/0/1 的类型为 trunk，允许所有 VLAN 通过。
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/1] quit
# 在接口 GigabitEthernet 1/0/2 上使能 PoE 为 AP 供电，类型为 Trunk，允许所有 VLAN 通过，且 PVID 设置为 100。
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] poe enable
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/2] port trunk pvid vlan 100
[SwitchB-GigabitEthernet1/0/2] quit
# 创建 VLAN168，并配置对应接口的 IP 地址，用来和无线客户端通信。
[SwitchB] vlan 168
[SwitchB-vlan168] quit
[SwitchB] interface vlan-interface 168
[SwitchB-Vlan-interface168] ip address 192.168.2.2 24
[SwitchB-Vlan-interface168] quit
# 配置与公网设备通信的静态路由，下一跳指向与 Router 直连的接口。
[SwitchB] ip route-static 0.0.0.0 0 192.100.1.3
```

#### 4.4.5 apcfg.txt 配置文件

```
# 配置 Portal 服务器地址为 8.1.1.50，并指定服务器对应的 url。
system-view
portal server pt ip 8.1.1.50 key simple 123456 url http://8.1.1.50:8080/portal
# 配置 portal 免认证规则 1，用来放行 AP 上开启 Portal 服务的接口能够与 Portal 服务器通信。
portal free-rule 1 source interface GigabitEthernet 1/0/1 destination any
# 配置移动需求 Portal 参数。
portal device-id beijing-ac-01
portal url-param include nas-id param-name vlan
portal url-param include user-mac des-encrypt param-name wlanusermac
```

```

portal url-param include nas-ip param-name wlanacip
portal url-param include ap-mac param-name wlanapmac
portal url-param include user-url param-name wlanfirsturl
portal url-param include user-ip param-name wlanuserip
portal url-param include ac-name param-name wlanacname
portal url-param include ssid
# 创建 VLAN 168 及其接口，并进入接口视图。
vlan 168
interface vlan 168
# 开启直接认证方式的 Portal 认证。
portal server pt method direct
# 配置接口发送 Portal 报文使用的源地址为 AC 的地址。
portal nas-ip 138.10.1.80
# 配置通过 WLAN 获取 Portal 用户信息。
portal host-check wlan
interface GigabitEthernet 1/0/1
port link-type trunk
port trunk permit vlan all

```

## 4.4.6 配置 Portal 服务器

### (1) 配置 Portal 服务

#### # 配置 Portal 服务器。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，使用缺省配置。

图15 Portal 服务器配置页面

The screenshot shows the H3C Intelligent Management Center (iMC) Portal Server Configuration page. The breadcrumb navigation path is highlighted: 用户 > 接入策略管理 > Portal服务管理 > 服务器配置.

**Portal服务器配置**

**基本信息**

日志级别 \*

**Portal Server**

报文请求超时时长(秒) \*  逃生心跳间隔时长(秒) \*

用户心跳间隔时长(分钟) \*  LB设备地址

LB设备IPv6地址

**Portal Web**

请求报文超时时长(秒) \*  交互报文编码

校验终端用户请求报文  使用缓存

HTTP心跳界面展示方式  HTTP心跳界面展示方式

Portal主页

#### # 增加 Portal 地址组。

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入 IP 地址组配置页面。点击<增加>按钮，进入增加 IP 地址组页面。

- 输入 IP 地址组名：wjh-pt；
- 输入起始地址：192.168.2.0；
- 输入终止地址：192.168.3.255；
- 选择 IP 地址组的类型为“NAT”；
- 输入 NAT 转换后的起始地址和终止地址都为 138.10.1.3；
- 其他采用默认配置，单击<确定>按钮完成操作。

图16 增加 IP 地址组配置页面

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组

增加IP地址组

|           |               |
|-----------|---------------|
| IP地址组名 *  | wjh-pt        |
| 起始地址 *    | 192.168.2.0   |
| 终止地址 *    | 192.168.3.255 |
| 业务分组      | 未分组           |
| 类型 *      | NAT           |
| 转换后起始地址 * | 138.10.1.3    |
| 转换后终止地址 * | 138.10.1.3    |

确定 取消

#### # 增加 Portal 设备。

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 输入设备名：wjh；
- 输入 IP 地址：即 AC 上配置的 portal bas-ip 地址，138.10.1.80；
- 输入密钥：123456，与 AC 上配置的 portal server 密钥一致；
- 其他采用默认配置，单击<确定>按钮完成操作。

图17 增加设备信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息 帮助

增加设备信息

设备信息

|          |            |               |             |
|----------|------------|---------------|-------------|
| 设备名 *    | wjh        | 业务分组 *        | 未分组         |
| 版本 *     | Portal 2.0 | IP地址 *        | 138.10.1.80 |
| 监听端口 *   | 2000       | 本地Challenge * | 否           |
| 认证重发次数 * | 0          | 下线重发次数 *      | 1           |
| 支持逃生心跳 * | 否          | 支持用户心跳 *      | 否           |
| 密钥 *     | .....      | 确认密钥 *        | .....       |
| 组网方式 *   | 三层         |               |             |
| 设备描述     |            |               |             |

确定 取消

# 增加端口组信息。


在 Portal 设备配置页面中的设备信息列表中，单击<端口组信息管理>按钮（“”图标），进入端口组信息配置页面。

图18 设备配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 加入收藏 帮助

设备信息查询

|      |  |      |  |
|------|--|------|--|
| 设备名  |  | 版本   |  |
| 下发结果 |  | 业务分组 |  |

查询 重置

增加

| 设备名 | 版本         | 业务分组 | IP地址        | 最近一次下发时间 | 下发结果 | 操作                                                                                                                                                                                                                                                                                                                                                      |
|-----|------------|------|-------------|----------|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wjh | Portal 2.0 | 未分组  | 138.10.1.80 |          | 未下发  |     |

共有1条记录，当前第1 - 1，第 1/1 页。

« < 1 > » 50

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 输入端口组名：w-group；
- 选择 IP 地址组：wjh-pt；
- “是否 NAT” 选项中选择 “是”；
- 其他采用默认配置，单击<确定>按钮完成操作。

图19 增加端口组信息

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 增加端口组信息

帮助

增加端口组信息

端口组名 \*

w-group

开始端口 \*

0

协议类型 \*

HTTP

是否NAT \*

否

认证方式 \*

CHAP认证

心跳间隔(分钟) \*

10

用户域名

无感知认证

不支持

页面推送策略

提示语言 \*

动态检测

终止端口 \*

zzzzzz

快速认证 \*

否

错误透传 \*

是

IP地址组 \*

wjh-pt

心跳超时(分钟) \*

30

端口组描述

客户端防破解 \*

否

缺省认证页面

确定

取消

(2) 配置接入服务

# 增加接入设备。

选择“用户”标签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入到设备配置页面。在接入设备列表中单击<增加>按钮，进入增加接入设备页面。

- 选择手工增加接入设备，添加 IP 地址为 138.10.1.80 的接入设备，与 AC 上 RADIUS 方案中的 nas-ip 一致；

图20 手工增加接入设备

手工增加接入设备

起始IP地址 \*

138.10.1.80

结束IP地址

备注

确定

取消

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”，该密码与 AC 配置 RADIUS 方案时的地址一致；
- 选择接入设备类型为“H3C(General)”；

- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图21 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \*

1812

计费端口 \*

1813

组网方式

不启用混合组网

业务类型

LAN接入业务

接入设备类型

H3C(General)

业务分组

未分组

共享密钥 \*

.....

确认共享密钥 \*

.....

接入设备分组

无

设备列表

选择手工增加全部清除

| 设备名称 | 设备IP地址      | 设备型号 | 备注 | 删除 |
|------|-------------|------|----|----|
|      | 138.10.1.80 |      |    |    |

共有1条记录。

确定取消

# 增加接入策略。

选择“用户”标签，单击导航树[接入策略管理/接入策略管理]菜单项，进入到接入策略配置页面。在接入策略列表中点击<增加>按钮。

- 接入策略名输入“wjh-portal”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。



图22 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

帮助

基本信息

接入策略名 \*

wjh-portal

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☒ 不启用 ☐ EAP证书认证 ☐ WAPI证书认证

认证证书类型

EAP-TLS认证

下发VLAN

下发用户组

☐ 下发User Profile

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Windows可溶解客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔(分钟) 30

自动重连次数 3

客户端最低版本 1.00-0120

违规处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式 ☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定

取消

# 增加接入服务。

选择“用户”标签，单击导航树[接入策略管理/接入服务管理]菜单项，进入到接入服务配置页面。在接入服务列表中点击<增加>按钮，进入增加接入服务页面。

- 服务名输入“wjh-portal”；
- 缺省接入策略“wjh-portal”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图23 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

|                                           |                                        |               |              |
|-------------------------------------------|----------------------------------------|---------------|--------------|
| 服务名 *                                     | wjh-portal                             | 服务后缀          |              |
| 业务分组 *                                    | 未分组                                    | 缺省接入策略 *      | wjh-portal ? |
| 缺省私有属性下发策略 *                              | 不使用 ?                                  | 缺省单帐号在线数量限制 * | 0            |
| 缺省单帐号最大绑定终端数 *                            | 0                                      |               |              |
| 服务描述                                      |                                        |               |              |
| <input checked="" type="checkbox"/> 可申请 ? | <input type="checkbox"/> Portal无感知认证 ? |               |              |

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | 优先级 | 修改 | 删除 |
|-------------|------|----------|-----|----|----|
| 未找到符合条件的记录。 |      |          |     |    |    |

确定 取消

(3) 增加接入用户。

选择“用户”标签，单击导航树中的[接入用户管理/接入用户]菜单项，进入到接入用户配置页面。在接入用户列表中点击<增加>按钮，进入增加接入用户页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“wjh-portal”；
- 输入证件号码“111111”；
- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图24 增加用户

增加用户

基本信息

|        |            |        |        |                                            |
|--------|------------|--------|--------|--------------------------------------------|
| 用户姓名 * | wjh-portal | 证件号码 * | 111111 | <input checked="" type="checkbox"/> 检查是否可用 |
| 通讯地址   |            | 电话     |        | ?                                          |
| 电子邮件   |            | 用户分组 * | 未分组    | ?                                          |

确定 取消

- 勾选接入服务“wjh-portal”；
- 单击<确定>按钮完成操作。

图25 增加接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

wjh-portal

选择

增加用户

帐号名 \*

wjh-portal

☐ 预开户用户

☐ 缺省BYOD用户

☐ MAC地址认证用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                            | 服务后缀 | 状态  | 分配IP地址 |
|------------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> wjh-portal |      | 可申请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

无线SSID

VLAN ID/内层VLAN ID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

MAC地址

IP地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

4.4.7 验证配置

无线客户端使用 SSID 为 portal-local 的无线服务模板上线。在浏览器输入 Portal 服务器网段的任一地址，弹出 Portal 认证页面，输入 Portal 服务器上设置的用户名和密码进行认证上线。

33

图26 用户上线



# 当 Portal 用户认证成功并上线之后，AC 会将用户规则下发到 AP 设备上，用户报文在 AP 上直接做转发。在 AC 上通过命令 **display portal user interface** 查看 Portal 用户成功上线。

```
<AC> display portal user interface Vlan-interface 168
```

```
Index:9
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode:stand-alone
```

```
MAC                IP                Vlan    Interface
```

```
-----
0021-631e-7911     192.168.2.100    168     Vlan-interface168
```

```
On interface Vlan-interface168:total 1 user(s) matched, 1 listed.
```

# 在 AP 上通过命令 **dis portal acl dynamic interface** 查看用户规则下发成功。

```
<ap1> display portal acl dynamic interface Vlan-interface ?
```

```
<1,168>  VLAN interface
```

```
<ap1> display portal acl dynamic interface Vlan-interface 168
```

```
IPv4 portal ACL rules on Vlan-interface168:
```

```
Rule 0
```

```
Inbound interface : all
```

```
Type                : dynamic
```

```
Action              : permit
```

```
Source:
```

```
IP                  : 192.168.2.100
```

```
Mask                : 255.255.255.255
```

```
MAC                 : 0021-631e-7911
```

```
Interface           : any
```

```
VLAN                : 168
```

```
Protocol             : 0
```

```
Destination:
```

```
IP                  : 0.0.0.0
```

```
Mask                : 0.0.0.0
```

Author ACL:  
Number : NONE

#### 4.4.8 配置文件

- SwitchA

```
#
vlan 10
#
vlan 138
#
interface Bridge-Aggregation4
    port link-type trunk
    port trunk permit vlan all
#
interface Vlan-interface10
    ip address 138.10.1.1 255.255.0.0
#
interface Vlan-interface138
    ip address 8.138.1.2 255.255.0.0
#
interface Ten-GigabitEthernet4/0/1
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan all
    port link-aggregation group 4
#
interface Ten-GigabitEthernet4/0/2
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan all
    port link-aggregation group 4
#
ip route-static 8.0.0.0 255.0.0.0 8.138.1.1
#
```

- AC

```
#
portal server pt ip 8.1.1.50 key simple 123456 url http://8.1.1.50:8080/portal
portal free-rule 1 source interface Bridge-Aggregation1 destination any
portal host-check wlan
#
wlan client learn-ipaddr enable
#
vlan 10
#
vlan 168
#
radius scheme portal
```

```

primary authentication 8.1.1.50
primary accounting 8.1.1.50
key authentication simple 123456
key accounting simple 123456
user-name-format without-domain
nas-ip 138.10.1.80
#
domain portal
authentication portal radius-scheme portal
authorization portal radius-scheme portal
accounting portal radius-scheme portal
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template servicel clear
ssid portal-local
bind WLAN-ESS 1
client forwarding-mode local
service-template enable
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan all
#
interface Vlan-interface10
ip address 138.10.1.80 255.255.0.0
#
interface Vlan-interface168
ip address 192.168.1.1 255.255.0.0
portal server pt method direct
portal domain portal
portal nas-ip 138.10.1.80
portal forwarding-mode local
#
interface Ten-GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan all
port link-aggregation group 1
#
interface WLAN-ESS1
port access vlan 168

```

```

#
wlan ap ap1 model WA2620E-AGN id 1
  serial-id 210235A42MB108000001
  map-configuration apcfg.txt
  radio 1
    channel 161
    service-template service1
    radio enable
  radio 2
#
ip route-static 0.0.0.0 0.0.0.0 138.10.1.1
#
arp-snooping enable
#
•   Router
#
nat address-group 1 138.10.1.3 138.10.1.3
#
acl number 3000
  rule 1 permit ip source 192.100.0.0 0.0.255.255
  rule 2 permit ip source 192.168.0.0 0.0.255.255
#
dhcp server ip-pool 100
  network 192.100.0.0 mask 255.255.0.0
  gateway-list 192.100.1.3
  option 43 hex 80070000 018A0A01 50
#
dhcp server ip-pool 168
  network 192.168.2.0 mask 255.255.255.0
  gateway-list 192.168.2.3
  dns-list 192.168.2.3
  dns-list 8.1.1.5
#
interface GigabitEthernet0/0
  port link-mode route
  nat outbound 3000 address-group 1
  ip address 138.10.1.3 255.255.0.0
  ip virtual-reassembly
#
interface GigabitEthernet0/1
  port link-mode route
#
interface GigabitEthernet0/1.100
  vlan-type dot1q vid 100
  ip address 192.100.1.3 255.255.0.0
#
interface GigabitEthernet0/1.168
  vlan-type dot1q vid 168

```

```

ip address 192.168.2.3 255.255.255.0
#
ip route-static 8.0.0.0 255.0.0.0 138.10.1.1
#
dhcp enable
#
• SwitchB
#
vlan 100
#
vlan 168
#
interface Vlan-interface100
ip address 192.100.1.2 255.255.0.0
#
interface Vlan-interface168
ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
description routeg0/1
port link-type trunk
port trunk permit vlan all
#
interface GigabitEthernet1/0/2
description ap-portal-local
port link-type trunk
port trunk permit vlan all
port trunk pvid vlan 100
poe enable
#
ip route-static 0.0.0.0 0.0.0.0 192.100.1.3
#

```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。



# 本地转发方式 IPv6 Portal 认证典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                               |    |
|-------------------------------|----|
| 1 简介.....                     | 1  |
| 2 配置前提 .....                  | 1  |
| 3 AC 为无线客户端集中分配地址方式配置举例 ..... | 1  |
| 3.1 组网需求 .....                | 1  |
| 3.2 配置思路 .....                | 2  |
| 3.3 配置注意事项.....               | 2  |
| 3.4 配置步骤 .....                | 2  |
| 3.4.1 配置 Switch A .....       | 2  |
| 3.4.2 配置 AC.....              | 3  |
| 3.4.3 配置 Router.....          | 6  |
| 3.4.4 配置 Switch B .....       | 6  |
| 3.4.5 apcfg.txt 配置文件 .....    | 7  |
| 3.4.6 配置 Portal server .....  | 8  |
| 3.5 验证配置 .....                | 14 |
| 3.6 配置文件 .....                | 15 |
| 4 分支机构独立为无线客户端分配地址配置举例.....   | 19 |
| 4.1 组网需求 .....                | 19 |
| 4.2 配置思路 .....                | 19 |
| 4.3 配置注意事项.....               | 20 |
| 4.4 配置步骤 .....                | 20 |
| 4.4.1 配置 Switch A .....       | 20 |
| 4.4.2 配置 AC.....              | 20 |
| 4.4.3 配置 Router.....          | 23 |
| 4.4.4 配置 Switch B .....       | 24 |
| 4.4.5 apcfg.txt 配置文件 .....    | 24 |
| 4.4.6 配置 Portal 服务器 .....     | 25 |
| 4.4.7 验证配置 .....              | 31 |
| 4.4.8 配置文件 .....              | 33 |
| 5 相关资料 .....                  | 36 |

# 1 简介

本文档介绍本地转发方式 IPv6 Portal 认证的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 Portal 特性。

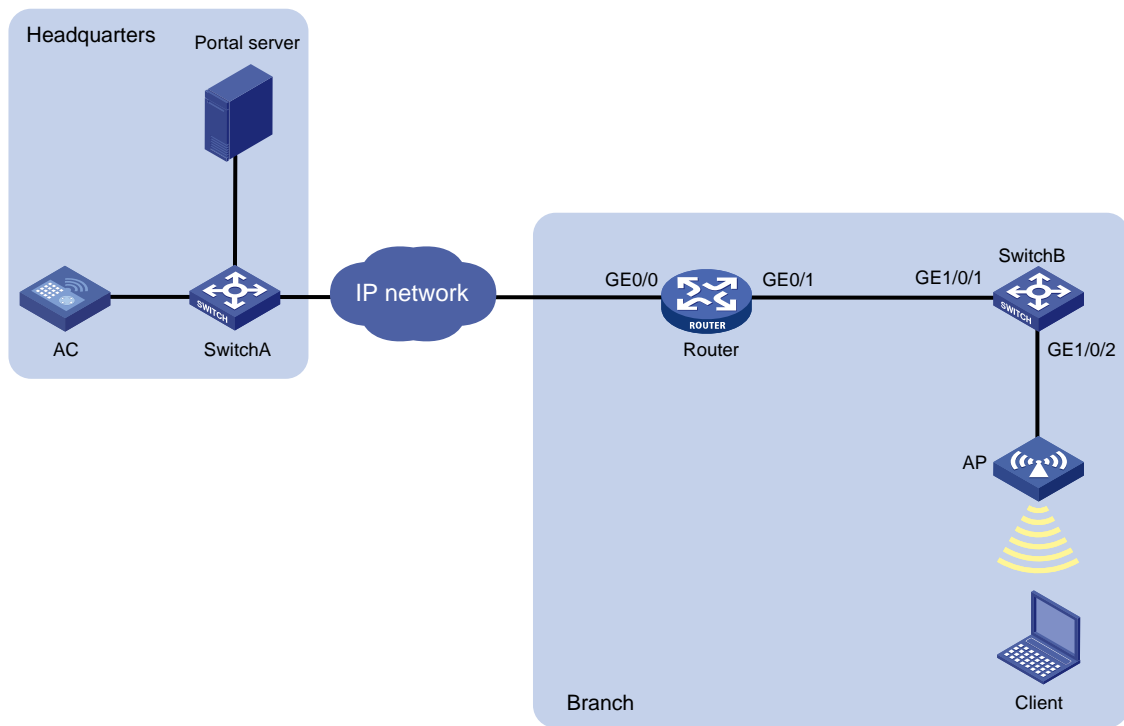
## 3 AC 为无线客户端集中分配地址方式配置举例

### 3.1 组网需求

如图 1 所示，总部的 AC 与分支机构的 AP 跨三层关联并作为 DHCPv6 server 为 Client 分配 IPv6 地址；Router 作为 Client 的网关并为 AP 分配 IPv6 地址，具体要求如下：

- 用户通过 Portal 认证接入无线网络；
- 用户通过 Portal 认证后，AC 将用户规则下发到 AP 上，用户报文在 AP 上直接做转发。

图1 AC 为无线客户端集中分配地址方式配置举例组网图



## 3.2 配置思路

- 为实现 AC 与 Portal 服务器通信，需要在 Switch A 上配置到 Portal 服务器的静态路由；
- 在 AC 上配置 DHCPv6 功能，使 AC 统一分配、集中管理各分支机构中无线客户端的地址；
- 为了使 AP 能够直接转发 Client 报文，需要在 AC 的服务模板下开启本地转发功能，同时通过下发 map-configuration 文件来对 AP 进行配置实现本地转发。
- 为了保证域名正常解析，需在 AC 和 AP 上配置免认证规则，放行 DNS 服务器地址（本例略）。

## 3.3 配置注意事项

- AC 上要配置从 WLAN 获取用户信息的功能；
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 配置 Switch A

# 创建 VLAN 10 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址，用来和 AC 通信。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 2001::50 64
[SwitchA-Vlan-interface10] quit
```

# 创建 VLAN 20 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址，用来和 AP 通信。

```
[SwitchA] vlan 20
[SwitchA-vlan20] quit
[SwitchA] interface vlan 20
[SwitchA-Vlan-interface20] ipv6 address 2004::50 64
[SwitchA-Vlan-interface20] quit
```

# 创建 VLAN 30 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址，用来和 Client 通信。

```
[SwitchA] vlan 30
[SwitchA-vlan30] quit
[SwitchA] interface vlan 30
[SwitchA-Vlan-interface30] ipv6 address 2003::50 64
[SwitchA-Vlan-interface30] quit
```

# 创建 VLAN 138 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址，用来和 Portal 服务器通信。

```
[SwitchA] vlan 138
[SwitchA-vlan138] quit
[SwitchA] interface vlan 138
[SwitchA-Vlan-interface138] ipv6 address 4000::1 64
[SwitchA-Vlan-interface138] quit
```

# 创建聚合口 4。

```
[SwitchA] interface bridge-aggregation 4
```

```
[SwitchA-Bridge-Aggregation4] quit
# 配置 SwitchA 与 AC 连接的接口加入聚合口 4。
[SwitchA] interface ten-gigabitethernet 4/0/1
[SwitchA-Ten-GigabitEthernet4/0/1] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/1] quit
[SwitchA] interface ten-gigabitethernet 4/0/2
[SwitchA-Ten-GigabitEthernet4/0/2] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/2] quit
# 配置聚合口为 Trunk 口，并允许所有 VLAN 通过。
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port link-type trunk
[SwitchA-Bridge-Aggregation4] port trunk permit vlan all
[SwitchA-Bridge-Aggregation4] quit
# 配置静态路由，用于 AC 与 Portal 服务器通信，下一跳指向与 Portal 服务器互通的网关。
[SwitchA] ipv6 route-static 4000:: 64 4000::2
```

### 3.4.2 配置 AC

#### (1) 配置 AC 接口

# 创建 VLAN 10 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址，AC 将使用该接口的 IPv6 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ipv6 address 2001::1 64
# 取消对 RA 消息发布的抑制。
[AC-Vlan-interface10] undo ipv6 nd ra halt
# 设置被管理地址配置标志位为 1。
[AC-Vlan-interface10] ipv6 nd autoconfig managed-address-flag
# 设置其他配置标志位为 1。
[AC-Vlan-interface10] ipv6 nd autoconfig other-flag
[AC-Vlan-interface10] quit
```

# 创建 VLAN 30 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址，用来作为 Client 接入的业务 VLAN。

```
[AC] vlan 30
[AC-vlan30] quit
[AC] interface vlan-interface 30
[AC-Vlan-interface30] ipv6 address 2003::1 64
# 取消对 RA 消息发布的抑制。
[AC-Vlan-interface30] undo ipv6 nd ra halt
# 设置被管理地址配置标志位为 1。
[AC-Vlan-interface30] ipv6 nd autoconfig managed-address-flag
# 设置其他配置标志位为 1。
[AC-Vlan-interface30] ipv6 nd autoconfig other-flag
```

```

[AC-Vlan-interface30] quit
# 创建聚合口 1。
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] quit
# 将 AC 上两个物理口加入聚合口 1。
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-aggregation group 1
[AC-GigabitEthernet1/0/1] quit
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] port link-aggregation group 1
[AC-GigabitEthernet1/0/2] quit
# 配置 AC 聚合口 1 的类型为 Trunk 口并允许所有 VLAN 通过，用来和 AP、Client 通信。
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] port link-type trunk
[AC-Bridge-Aggregation1] port trunk permit vlan all
[AC-Bridge-Aggregation1] quit
(2) 配置 DHCP 服务
# 使能 DHCPv6 服务器功能。
[AC] ipv6 dhcp server enable
# 创建 DHCPv6 地址池 30，用于为 Client 动态分配地址。
[AC] ipv6 dhcp pool 30
[AC-dhcp6-pool-30] network 2003::/64
[AC-dhcp6-pool-30] quit
[AC] interface vlan-interface 30
[AC-Vlan-interface30] ipv6 dhcp server apply pool 30
[AC-Vlan-interface30] quit
(3) 配置 WLAN-ESS 接口
# 创建接口 WLAN-ESS 30。
[AC] interface wlan-ess 30
# 配置端口的链路类型为 Access，允许 VLAN 30 通过。
[AC-WLAN-ESS30] port access vlan 30
[AC-WLAN-ESS30] quit
(4) 配置无线服务模板
# 创建 clear 类型的无线服务模板 1。
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 portal-local。
[AC-wlan-st-1] ssid portal-local
# 将 WLAN-ESS30 接口绑定到无线服务模板 1。
[AC-wlan-st-1] bind wlan-ess 30
# 开启用户本地转发功能。
[AC-wlan-st-1] client forwarding-mode local
# 使能无线服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit

```

(5) 在 AC 下绑定无线服务模板

# 创建 AP 模板，名称为 ap1，型号名称选择 WA2620E-AGN，并配置其序列号。

```
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 210235A42MB108000002
[AC-wlan-ap-ap1] map-configuration apcfg.txt
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-ap1] radio 1
# 将无线服务模板 1 绑定到 AP 的 radio 1 口。
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

(6) 配置 Portal 认证

# 配置 Portal 认证服务器地址为 4000::50，并指定服务器对应的 URL。

```
[AC] portal server pt ipv6 4000::50 key simple 123456 url http://[4000::50]:8080/portal
```

# 配置 Portal 免认证规则 1，用来放行 AC 上配置 Portal 认证服务的接口能够与 Portal 服务器通信。

```
[AC] portal free-rule 1 source interface bridge-aggregation1 destination any
```

# 配置 AC 通过 WLAN 获取 Portal 用户信息。

```
[AC] portal host-check wlan
```

# 配置 RADIUS 方案 portal。

```
[AC] radius scheme portal
```

# 配置认证、计费 and 授权服务器的 IPv6 地址为 4000::50。

```
[AC-radius-portal] primary authentication ipv6 4000::50
[AC-radius-portal] primary accounting ipv6 4000::50
```

# 配置与认证、计费 and 授权服务器交互报文时的共享密钥为 123456。

```
[AC-radius-portal] key authentication simple 123456
[AC-radius-portal] key accounting simple 123456
```

# 指定发送给 RADIUS 服务器的用户名不携带域名。

```
[AC-radius-portal] user-name-format without-domain
```

# 配置设备发送 RADIUS 报文使用的源 IPv6 地址为 2001::1。

```
[AC-radius-portal] nas-ip ipv6 2001::1
[AC-radius-portal] quit
```

# 配置 AAA 认证域 portal。

```
[AC] domain portal
```

# 设置 ISP 域的认证、授权和计费方法均为 RADIUS。

```
[AC-isp-portal] authentication portal radius-scheme portal
[AC-isp-portal] accounting portal radius-scheme portal
[AC-isp-portal] authorization portal radius-scheme portal
[AC-isp-portal] quit
```

# 配置接口 VLAN 30 为 Portal 直接认证的接口。

```
[AC] interface vlan-interface 30
[AC-Vlan-interface30] portal server pt method direct
```

# 指定从接口接入的 IPv6 Portal 用户使用认证域为 portal。

```
[AC-Vlan-interface30] portal domain ipv6 portal
```

```
# 配置接口发送 Portal 报文使用的 IPv6 源地址为 2001::1。
[AC-Vlan-interface30] portal nas-ip ipv6 2001::1
# 开启 Portal 本地转发功能。
[AC-Vlan-interface30] portal forwarding-mode local
# 配置 Portal 用户报文的控制模式为 MAC。
[AC-Vlan-interface30] portal control-mode mac
[AC-Vlan-interface30] quit
# 配置 AC 与 AP 和 Portal 服务器通信的静态路由下一跳为 Switch A 的接口 VLAN 10。
[AC] ipv6 route-static :: 0 2001::50
```

### 3.4.3 配置 Router

```
# 配置 GigabitEthernet0/0 的 IPv6 地址，用来和 AC 通信。
<Router> system-view
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] ipv6 address 2001::3 64
[Router-GigabitEthernet0/0] quit
# 配置 GigabitEthernet0/1 的 IPv6 地址。
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] ipv6 address 2004::3 64
[Router-GigabitEthernet0/1] quit
# 使能 DHCPv6 服务器功能。
[Router] ipv6 dhcp server enable
# 配置 DHCP 地址池 20，用于为 AP 动态分配地址。
[Router] ipv6 dhcp pool 20
[Router-dhcp6-pool-20] network 2004::/64
[Router-dhcp6-pool-20] option 52 hex 20010000000000000000000000000001
[Router-dhcp6-pool-20] quit
# 配置接口 GigabitEthernet0/1 工作在 DHCPv6 服务器模式，引用地址池 20。
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] ipv6 dhcp server apply pool 20
[Router-GigabitEthernet0/1] quit
# 配置 Router 到公网的静态路由，下一跳指向 AC 交换侧的地址。
[Router] ipv6 route-static :: 0 2001::1
```

### 3.4.4 配置 Switch B

```
# 创建 VLAN 20，并配置对应接口 IPv6 地址，用来和 Router 通信。
<SwitchB> system-view
[SwitchB] vlan 20
[SwitchB-vlan20] quit
[SwitchB] interface vlan-interface 20
[SwitchB-Vlan-interface20] ipv6 address 2004::2 64
[SwitchB-Vlan-interface20] quit
# 配置 GigabitEthernet1/0/1 的类型为 Trunk，允许所有 VLAN 通过。
[SwitchB] interface gigabitethernet 1/0/1
```



```
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/1] quit
# 配置 GigabitEthernet1/0/2 接口属性, 使能 PoE 为 AP 供电, 类型为 Trunk, 允许所有 VLAN 通过, 且 PVID 设置为 20。
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] poe enable
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/2] port trunk pvid vlan 20
[SwitchB-GigabitEthernet1/0/2] quit
# 创建 VLAN 30, 并配置对应接口的 IPv6 地址, 用来和无线客户端通信。
[SwitchB] vlan 30
[SwitchB-vlan30] quit
[SwitchB] interface vlan-interface 30
[SwitchB-Vlan-interface30] ipv6 address 2003::2 64
[SwitchB-Vlan-interface30] quit
# 配置与公网设备通信的静态路由, 下一跳指向与 Router 直连的接口。
[SwitchB] ipv6 route-static :: 0 2004::3
```

### 3.4.5 apcfg.txt 配置文件

```
# 配置 Portal 服务器地址为 4000::50, 并指定服务器对应的 url。
system-view
portal server pt ipv6 4000::50 key simple 123456 url http://[4000::50]:8080/portal
# 配置 Portal 免认证规则 1, 用来放行 AP 上开启 Portal 认证服务的接口能够与 Portal 服务器通信。
portal free-rule 1 source interface GigabitEthernet 1/0/1 destination any
# 配置移动需求的 Portal 参数。
portal device-id beijing-ac-01
portal url-param include nas-id param-name vlan
portal url-param include user-mac des-encrypt param-name wlanusermac
portal url-param include nas-ip param-name wlanacip
portal url-param include ap-mac param-name wlanapmac
portal url-param include user-url param-name wlanfirsturl
portal url-param include user-ip param-name wlanuserip
portal url-param include ac-name param-name wlanacname
portal url-param include ssid
portal host-check wlan
# 创建 vlan 30。
vlan 30
# 创建 VLAN 30 对应接口, 并进入接口 VLAN 30 视图
interface vlan 30
# 接口下指定 Portal 服务器并配置为直接认证方式。
portal server pt method direct
# 配置接口发送 Portal 报文使用的源地址为 AC 的地址。
portal nas-ip ipv6 2001::1
```

# 配置 Portal 用户报文的控制模式为 MAC。

```
portal control-mode mac
```

# 进入到 AP 的物理接口 GigabitEthernet1/0/1。

```
interface GigabitEthernet 1/0/1
```

# 配置接口 GigabitEthernet1/0/1 类型为 Trunk。

```
port link-type trunk
```

# 配置接口 GigabitEthernet1/0/1 允许所有 VLAN 通过。

```
port trunk permit vlan all
```

### 3.4.6 配置 Portal server



说明

下面以 iMC 为例(使用 iMC 版本为: iMC PLAT 7.1 (E0303)、iMC EAD 7.1 (E0303), 说明 RADIUS server 的基本配置。

#### (1) 配置 Portal 服务

# 配置 Portal 服务器。

登录进入 iMC 管理平台, 选择“用户”页签, 单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项, 进入服务器配置页面, 使用缺省配置。

图2 Portal 服务器配置页面

The screenshot displays the 'Portal 服务器配置' (Portal Server Configuration) page in the iMC Intelligent Management Center. The page is divided into two main sections: 'Portal Server' and 'Portal Web'. The 'Portal Server' section includes fields for '日志级别' (Log Level) set to '警告' (Warning), '报文请求超时时长(秒)' (Request Timeout) set to 15, '用户心跳间隔时长(分钟)' (User Session Timeout) set to 3, and 'LB设备地址' (LB Device Address). The 'Portal Web' section includes fields for '请求报文超时时长(秒)' (Request Timeout) set to 15, '交互报文编码' (Authentication Code), and '使用缓存' (Use Cache) set to '是' (Yes). The 'HTTP心跳界面展示方式' (HTTP Session Display Mode) is set to '新页面' (New Page). At the bottom, there is a list of 'Portal/主页' (Portal/Homepage) URLs.

# 配置 IP 地址组。

选择“用户”页签, 单击导航树[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项, 进入 IP 地址组配置页面, 在该页面中单击<增加>按钮, 进入增加 IP 地址组配置页面。

- 输入 IP 地址组名: wjh-pt;
- IPv6 选择“是”;
- 输入起始地址: 2003::1;

- 输入终止地址：2003::255；
- 其他采用缺省配置，单击<确定>按钮完成操作。

图3 增加 IP 地址组配置页面

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组

增加IP地址组

IP地址组名 \* wjh-pt

IPv6 \* 是

起始地址 \* 2003::1

终止地址 \* 2003::255

业务分组 未分组

确定 取消

#### # 增加 Portal 设备。

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入设备配置页面。在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 输入设备名：wjh；
- 输入 IP 地址：即 AC 上配置的 portal bas-ip 地址，2001::1；
- 输入密钥：123456，与 AC 上配置的 Portal server 密钥一致；
- 其他采用默认配置，单击<确定>按钮完成操作。

图4 增加设备信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

增加设备信息

设备信息

设备名 \* wjh

版本 \* Portal 3.0

监听端口 \* 2000

认证重发次数 \* 0

支持逃生心跳 \* 否

密钥 \* \*\*\*\*\*

组网方式 \* 直连

设备描述

业务分组 \* 未分组

IP地址 \* 2001::1

本地Challenge \* 否

下线重发次数 \* 1

支持用户心跳 \* 否

确认密钥 \* \*\*\*\*\*

确定 取消

#### # 增加端口组信息。


在 Portal 设备配置页面中的设备信息列表中，单击<端口组信息管理>按钮（“”图标），进入端口组信息配置页面。

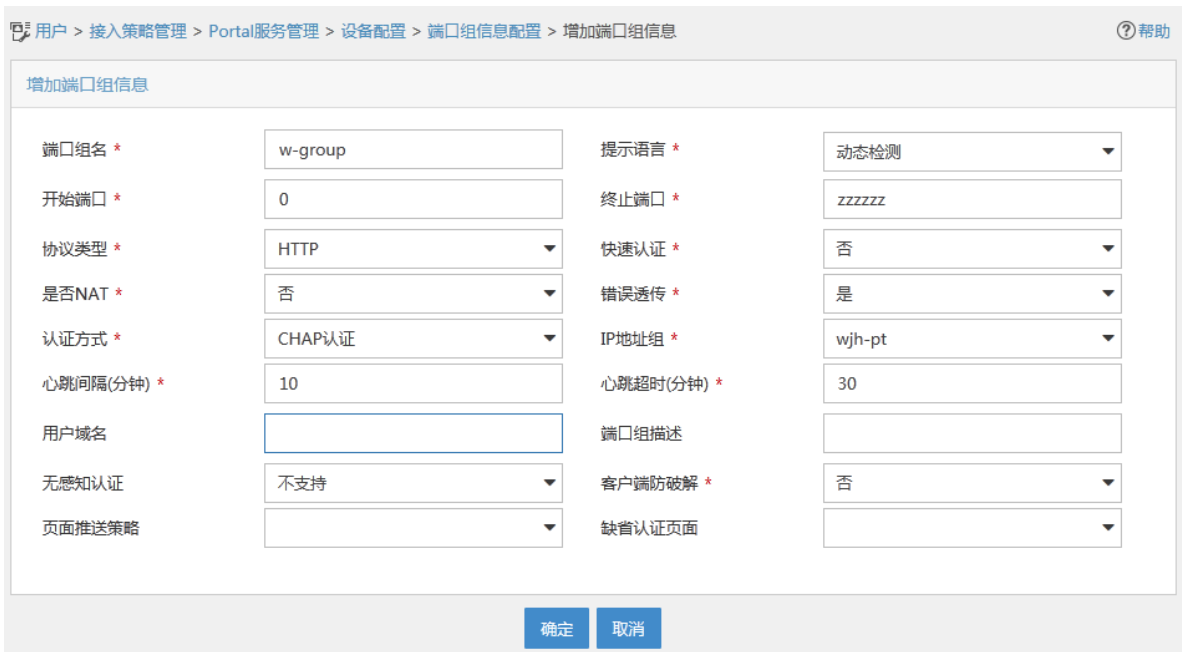
图5 设备配置页面



在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 输入端口组名：w-group；
- 选择 IP 地址组：wjh-pt；
- 其他采用默认配置，单击<确定>按钮完成操作。

图6 增加端口组信息



(2) 配置接入服务

# 增加接入设备

选择“用户”标签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面。在该页面中单击<增加>按钮，进入增加接入设备页面。

选择手工增加接入设备，添加 IPv6 地址为 2001::1 的接入设备，与 AC 上 RADIUS 方案中的 nas-ip 一致；

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”，该密码与 AC 配置 RADIUS 方案时的地址一致；
- 选择接入设备类型为“H3C(General)”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图7 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

接入配置

认证端口 \*

1812

组网方式

不启用混合组网

接入设备类型

H3C(General)

共享密钥 \*

\*\*\*\*\*

接入设备分组

无

计费端口 \*

1813

业务类型

LAN接入业务

业务分组

未分组

确认共享密钥 \*

\*\*\*\*\*

设备列表

选择手工增加增加IPv6设备全部清除

| 设备名称 | 设备IP地址                             | 设备型号 | 备注 | 删除 |
|------|------------------------------------|------|----|----|
|      | 2001:0000:0000:0000:0000:0000:0001 |      |    | 删除 |

共有1条记录。

确定取消

# 增加接入策略。

选择“用户”标签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略配置页面。在接入策略列表中单击<增加>按钮，进入增加接入策略页面。

- 接入策略名输入“wjh-portal”；
- 业务分组“未分组”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

帮助

基本信息

接入策略名 \*

wjh-portal

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☒ 不启用 ☐ EAP证书认证 ☐ WAPI证书认证

认证证书类型

EAP-TLS认证

下发VLAN

下发用户组

☐ 下发User Profile

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Windows可溶解客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔(分钟) 30

自动重连次数 3

客户端最低版本 1.00-0120

违规处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式 ☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定

取消

# 增加接入服务。

选择“用户”标签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务配置页面。在接入服务列表中点击<增加>按钮。

- 服务名输入“wjh-portal”；
- 缺省接入策略“wjh-portal”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 \*

wjh-portal

业务分组 \*

未分组

服务后缀

缺省接入策略 \*

wjh-portal

缺省私有属性下发策略 \*

不使用

缺省单帐号最大绑定终端数 \*

0

缺省单帐号在线数量限制 \*

0

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | 优先级 | 修改 | 删除 |
|-------------|------|----------|-----|----|----|
| 未找到符合条件的记录。 |      |          |     |    |    |

确定

取消

(3) 增加接入用户。

# 选择“用户”标签，单击导航树中的[接入用户管理/接入用户]菜单项，进入到接入用户配置页面。在接入用户列表中点击<增加>按钮，进入增加接入用户页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“wjh-portal”；
- 输入证件号码“111111”；
- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图10 增加用户

增加用户

基本信息

用户姓名 \*

wjh-portal

✓

证件号码 \*

111111

✓

检查是否可用

通讯地址

电话

?

电子邮件

?

用户分组 \*

未分组

确定

取消

- 账号名输入“wjh-portal”；
- 勾选接入服务“wjh-portal”；

- 单击<确定>按钮完成操作。

图11 增加接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

wjh-portal

选择

增加用户

帐号名 \*

wjh-portal

☐ 预开户用户

☐ 缺省BYOD用户

☐ MAC地址认证用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                            | 服务后缀 | 状态  | 分配IP地址 |
|------------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> wjh-portal |      | 可申请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线SSID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

IP地址

MAC地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

### 3.5 验证配置

- # 无线客户端使用 SSID 为 portal-local 的无线服务模板上线，获取到地址。在浏览器中输入 Portal 服务器网段的任一地址，弹出 Portal 认证页面，输入 Portal 服务器上设置的用户名和密码进行认证上线。
- # 当 Portal 用户认证成功并上线之后，AC 会将用户规则下发到 AP 设备上，用户报文在 AP 上直接做转发。在 AC 上通过命令 **display portal user interface** 查看成功上线的用户。



```
<AC> display portal user interface vlan 30
Index:0
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC                IP                Vlan  Interface
-----
0021-631e-7911    2003::1          30    Vlan-interface10
On interface Vlan-interface10:total 1 user(s) matched, 1 listed.
```

# 在 AP 上通过命令 **display portal acl dynamic interface** 查看用户规则成功下发。

```
<ap1> display portal acl dynamic interface vlan-interface 30
IPv4 portal ACL rules on Vlan-interface10:
Rule 0
Inbound interface : all
Type              : dynamic
Action            : permit
Source:
  IP               : 2003::1
  Mask             : 255.255.255.255
  MAC              : 0021-631e-7911
  Interface        : any
  VLAN             : 30
  Protocol         : 0
Destination:
  IP               : 0.0.0.0
  Mask             : 0.0.0.0
Author ACL:
  Number          : NONE
```

## 3.6 配置文件

- SwitchA

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 138
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan all
#
interface Vlan-interface10
```

```

    ipv6 address 2001::50 64
#
interface Vlan-interface20
    ipv6 address 2004::50 64
#
interface Vlan-interface30
    ipv6 address 2003::50 64
#
interface Vlan-interface138
    ipv6 address 4000::1 64
#
interface Ten-GigabitEthernet4/0/1
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan all
    port link-aggregation group 4
#
interface Ten-GigabitEthernet4/0/2
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan all
    port link-aggregation group 4
#
    ipv6 route-static 4000:: 64 4000::2
#

```

## - AC

```

#
    portal server pt ipv6 4000::50 key cipher $c$3$rNRhle2UN3+u8va/OYD8LNQIHpTspvL5ng== url
http://[4000::50]:8080/portal server-type imc
    portal free-rule 1 source interface Bridge-Aggregation1 destination any
    portal host-check wlan
#
    ipv6 dhcp server enable
#
vlan 10
#
vlan 30
#
radius scheme portal
    primary authentication ipv6 4000::0050
    primary accounting ipv6 4000::0050
    key authentication cipher $c$3$M3465DvHOI26Az+zawNZzuig0Nbyao4mJg==
    key accounting cipher $c$3$9dX0xsAmXke7pEK0DpfAlwlcBecKrjYxVQ==
    user-name-format without-domain
    nas-ip ipv6 2001::0001
#
domain portal
    authentication portal radius-scheme portal

```

```

authorization portal radius-scheme portal
accounting portal radius-scheme portal
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 clear
ssid portal-local
bind WLAN-ESS 30
client forwarding-mode local
service-template enable
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan all
#
interface Vlan-interface10
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
ipv6 address 2001::1/64
#
interface Vlan-interface30
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
ipv6 address 2003::1/64
ipv6 dhcp server apply pool 30
portal control-mode mac
portal server pt method direct
portal domain ipv6 portal
portal nas-ip ipv6 2001::1
portal forwarding-mode local
#
interface Ten-GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan all
port link-aggregation group 1
#
interface WLAN-ESS30
port access vlan 30
#

```

```
wlan ap ap1 model WA2620E-AGN id 1
serial-id 210235A42MB108000002
radio 1
service-template 1
radio enable
radio 2
```

```
#
ipv6 route-static :: 0 2001::50
```

```
#
```

## ● Router

```
#
ipv6 dhcp server enable
#
ipv6 dhcp pool 20
network 2004::/64
option 52 hex 20010000000000000000000000000001
```

```
#
```

```
interface GigabitEthernet0/0
port link-mode route
ipv6 address 2001::3 64
```

```
#
```

```
interface GigabitEthernet0/1
port link-mode route
ipv6 address 2004::3 64
ipv6 dhcp server apply pool 20
```

```
#
```

```
ipv6 route-static :: 0 2001::1
```

```
#
```

## ● SwitchB

```
#
```

```
vlan 20
```

```
#
```

```
vlan 30
```

```
#
```

```
interface Vlan-interface20
ipv6 address 2004::2 64
```

```
#
```

```
interface Vlan-interface30
ipv6 address 2003::2 64
```

```
#
```

```
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
```

```
#
```

```
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan all
port trunk pvid vlan 20
```

```

poe enable
#
ipv6 route-static :: 0 2004::3
#

```

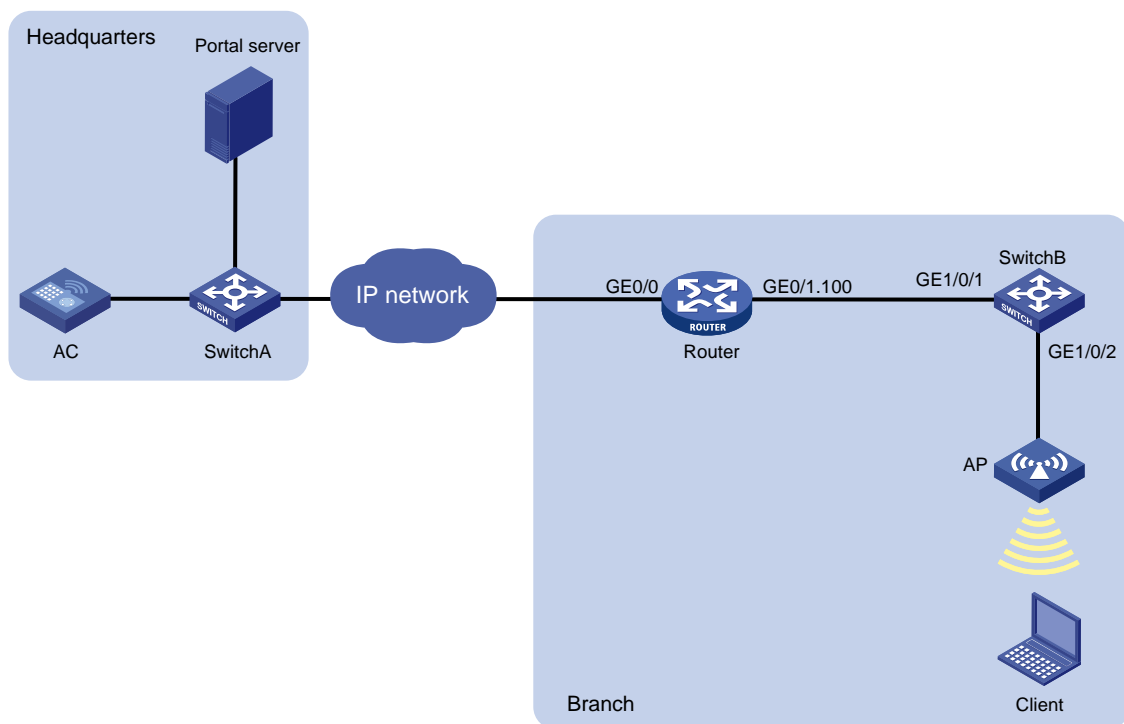
## 4 分支机构独立为无线客户端分配地址配置举例

### 4.1 组网需求

如图 12 所示，总部的 AC 与分支机构的 AP 跨三层关联；Router 作为无线客户端的网关并为 AP 分配地址，具体要求如下：

- 用户通过 Portal 认证接入无线网络；
- 用户通过 Portal 认证后，AC 将用户规则下发到 AP 上，用户报文在 AP 上直接做转发。
- 各分支机构无线客户端的地址由各分支机构单独分配。

图12 分支机构独立分配无线客户端地址的组网图



### 4.2 配置思路

- 为实现 AC 与 Portal 服务器通信，Switch A 上配置 AC 与 Portal 服务器通信的静态路由。
- 为避免各分支机构中的无线客户端地址重复，Router 上配置为无线客户端分配地址的地址池。
- 为了使 AP 能够直接转发 Client 报文，需要在 AC 的无线服务模板上开启本地转发功能，同时通过下发 map-configuration 文件来对 AP 进行配置实现本地转发。

## 4.3 配置注意事项

- AC上要配置用户信息从WLAN获取的功能。
- 配置AP的序列号时请确保该序列号与AP唯一对应,AP的序列号可以通过AP设备背面的标签获取。

## 4.4 配置步骤

### 4.4.1 配置 Switch A

# 创建 VLAN 10 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址用来和 AC 通信。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface vlan 10
[SwitchA-Vlan-interface10] ipv6 address 2001::50 64
[SwitchA-Vlan-interface10] quit
```

# 创建 VLAN 138 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址用来和 Portal 服务器通信。

```
[SwitchA] vlan 138
[SwitchA-vlan138] quit
[SwitchA] interface vlan 138
[SwitchA-Vlan-interface138] ipv6 address 4000::1 64
[SwitchA-Vlan-interface138] quit
```

# 创建聚合口 4。

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] quit
```

# 配置 SwitchA 与 AC 连接的接口加入聚合口。

```
[SwitchA] interface ten-gigabitethernet 4/0/1
[SwitchA-Ten-GigabitEthernet4/0/1] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/1] quit
[SwitchA] interface ten-gigabitEthernet 4/0/2
[SwitchA-Ten-GigabitEthernet4/0/2] port link-aggregation group 4
[SwitchA-Ten-GigabitEthernet4/0/2] quit
```

# 配置聚合口为 Trunk 口，并允许所有 VLAN 通过。

```
[SwitchA] int bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port link-type trunk
[SwitchA-Bridge-Aggregation4] port trunk permit vlan all
[SwitchA-Bridge-Aggregation4] quit
```

# 配置静态路由，用于 Portal 服务器与 AC 之间通信，下一跳指向和 Portal 服务器互通的网关。

```
[SwitchA] ipv6 route-static 4000:: 64 4000::2
```

### 4.4.2 配置 AC

#### (1) 配置 AC 接口

# 创建 VLAN 10 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址用来和 Portal 服务器通信。

```
<AC> system-view
```

```

[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ipv6 address 2001::1 64
[AC-Vlan-interface10] quit
# 创建 VLAN 168 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址用来配置 Portal 服务。
[AC] vlan 168
[AC-vlan168] quit
[AC] interface vlan-interface 168
[AC-Vlan-interface168] ipv6 address 4000::3 64
[AC-Vlan-interface168] quit
# 创建聚合口 1。
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] quit
# 将 AC 上两个物理口加入聚合口 1。
[AC] interface ten-gigabitethernet 1/0/1
[AC-Ten-GigabitEthernet1/0/1] port link-aggregation group 1
[AC-Ten-GigabitEthernet1/0/1] quit
[AC] interface ten-gigabitethernet 1/0/2
[AC-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
[AC-Ten-GigabitEthernet1/0/2] quit
# 配置 AC 聚合口 1 的类型为 Trunk 口并允许所有 VLAN 通过。
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] port link-type trunk
[AC-Bridge-Aggregation1] port trunk permit vlan all
[AC-Bridge-Aggregation1] quit
(2) 配置 WLAN-ESS 接口
# 创建接口 WLAN-ESS 1。
[AC] interface wlan-ess 1
# 配置端口的链路类型为 Access，允许 VLAN 168 通过。
[AC-WLAN-ESS1] port access vlan 168
[AC-WLAN-ESS1] quit
(3) 配置无线服务模板
# 创建 clear 类型的服务模板 1。
[AC] wlan service-template 1 clear
# 设置无线服务模板的 SSID 为 portal-local。
[AC-wlan-st-1] ssid portal-local
# 将 WLAN-ESS 1 接口绑定到无线服务模板。
[AC-wlan-st-1] bind wlan-ess 1
# 开启用户本地转发功能。
[AC-wlan-st-1] client forwarding-mode local
# 使能无线服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(4) 在 AC 下绑定无线服务模板

```

# 创建 AP 模板，名称为 ap1，型号名称选择 WA2620E-AGN，并配置其序列号。

```
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 210235A42MB108000001
[AC-wlan-ap-ap1] map-configuration apcfg.txt
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-ap1] radio 1
# 将服务模板 1 绑定到 AP 的 radio 1 口。
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

## (5) 配置 Portal 认证

# 配置 Portal 服务器地址为 4000::50，并指定服务器对应的 url。

```
[AC] portal server pt ipv6 4000::50 key simple 123456 url http://[4000::50]:8080/portal
```

# 配置 Portal 免认证规则 1，用于放行 AC 上起 Portal 的接口能够与 Portal 服务器通信。

```
[AC] portal free-rule 1 source interface Bridge-Aggregation1 destination any
```

# 配置 AC 通过 WLAN 来获取 Portal 用户的相关信息。

```
[AC] portal host-check wlan
```

# 配置 RADIUS 方案 portal。

```
[AC] radius scheme portal
```

# 配置认证、计费 and 授权服务器的 IPv6 地址为 4000::50。

```
[AC-radius-portal] primary authentication ipv6 4000::50
[AC-radius-portal] primary accounting ipv6 4000::50
```

# 配置与认证、计费 and 授权服务器交互报文时的共享密钥均为 123456。

```
[AC-radius-portal] key authentication simple 123456
[AC-radius-portal] key accounting simple 123456
```

# 指定发送给 RADIUS 方案 portal 中 RADIUS 服务器的用户名不携带域名。

```
[AC-radius-portal] user-name-format without-domain
```

# 配置设备发送 RADIUS 报文使用的源 IPv6 地址为 2001::1。

```
[AC-radius-portal] nas-ip ipv6 2001::1
[AC-radius-portal] quit
```

# 配置 AAA 认证域 portal。

```
[AC] domain portal
```

# 设置 ISP 域的认证、授权和计费方法均为 RADIUS 方式。

```
[AC-isp-portal] authentication portal radius-scheme portal
[AC-isp-portal] accounting portal radius-scheme portal
[AC-isp-portal] authorization portal radius-scheme portal
[AC-isp-portal] quit
```

# 在接口 VLAN 168 上开启 Portal 直接认证。

```
[AC] interface vlan-interface 168
[AC-Vlan-interface168] portal server pt method direct
```

# 指定从接口接入的 IPv6 Portal 用户使用认证域为 portal。

```
[AC-Vlan-interface168] portal domain ipv6 portal
```

# 配置接口发送 Portal 报文使用的 IPv6 源地址为 2001::1。



```
[AC-Vlan-interface168] portal nas-ip ipv6 2001::1
# 开启 Portal 本地转发功能。
[AC-Vlan-interface168] portal forwarding-mode local
# 配置 Portal 用户报文的控制模式为 MAC。
[AC-Vlan-interface168] portal control-mode mac
[AC-Vlan-interface168] quit
# 配置与 Portal 服务器等公网设备通信的静态路由。
[AC] ip route-static :: 0 2001::2
```

#### 4.4.3 配置 Router

```
# 配置接口 GigabitEthernet 0/0 的 IPv6 地址，用来与 AC 通信。
<Router> system-view
[Router] interface gigabitethernet 0/0
[Router-GigabitEthernet0/0] ipv6 address 2001::3 64
[Router-GigabitEthernet0/0] quit
# 创建子接口 GigabitEthernet 0/1.100，并配置 IPv6 地址，划分 VLAN 为 100，用来与 AP 通信。
[Router] interface gigabitethernet 0/1.100
[Router-GigabitEthernet0/1.100] ipv6 address 2004::3 64
[Router-GigabitEthernet0/1.100] vlan-type dot1q vid 100
[Router-GigabitEthernet0/1.100] quit
# 创建子接口 GigabitEthernet 0/1.168，并配置 IPv6 地址，划分 VLAN 为 168，用来与无线客户端通信。
[Router] interface gigabitethernet 0/1.168
[Router-GigabitEthernet0/1.168] ipv6 address 2003::1 64
[Router-GigabitEthernet0/1.168] vlan-type dot1q vid 168
[Router-GigabitEthernet0/1.168] quit
# 使能 DHCPv6 服务器功能。
[Router] ipv6 dhcp server enable
# 配置 DHCPv6 地址池 100，用来为 AP 分配 IPv6 地址。
[Router] ipv6 dhcp pool 100
[Router-dhcp6-pool-100] network 2004::/64
[Router-dhcp6-pool-100] quit
# 配置 DHCPv6 地址池 168，用于为无线客户端分配 IPv6 地址。
[Router] ipv6 dhcp pool 168
[Router-dhcp6-pool-168] network 2003::/64
[Router-dhcp6-pool-168] quit
# 配置接口 GigabitEthernet0/1.100 工作在 DHCPv6 服务器模式，引用地址池 100。
[Router] interface gigabitethernet 0/1.100
[Router-GigabitEthernet0/1.100] ipv6 dhcp server apply pool 100
[Router-GigabitEthernet0/1.100] quit
# 配置接口 GigabitEthernet0/1.168 工作在 DHCPv6 服务器模式，引用地址池 168。
[Router] interface gigabitethernet 0/1.168
[Router-GigabitEthernet0/1.168] ipv6 dhcp server apply pool 168
[Router-GigabitEthernet0/1.168] quit
# 配置 Router 到 Portal 服务器的静态路由，下一跳指向 AC 交换侧的地址。
```

```
[Router] ipv6 route-static 4000:: 64 2001::2
```

#### 4.4.4 配置 Switch B

# 创建 VLAN 100，并配置对应接口 IPv6 地址，用来和 Router 通信。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ipv6 address 2001::3 64
[SwitchB-Vlan-interface100] quit
```

# 配置接口 GigabitEthernet 1/0/1 的类型为 trunk，允许所有 VLAN 通过。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/1] quit
```

# 在接口 GigabitEthernet 1/0/2 上使能 PoE 为 AP 供电，类型为 Trunk，允许所有 VLAN 通过，且 PVID 设置为 100。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] poe enable
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/2] port trunk pvid vlan 100
[SwitchB-GigabitEthernet1/0/2] quit
```

# 创建 VLAN168，并配置对应接口的 IPv6 地址，用来和无线客户端通信。

```
[SwitchB] vlan 168
[SwitchB-vlan168] quit
[SwitchB] interface vlan-interface 168
[SwitchB-Vlan-interface168] ipv6 address 2004::2 64
[SwitchB-Vlan-interface168] quit
```

# 配置与公网设备通信的静态路由，下一跳指向与 Router 直连的接口。

```
[SwitchB] ip route-static :: 0 2004::3
```

#### 4.4.5 apcfg.txt 配置文件

# 配置 Portal 服务器地址为 4000::50，并指定服务器对应的 url。

```
system-view
portal server pt ipv6 4000::50 key simple 123456 url http://[4000::50]:8080/portal
```

# 配置 portal 免认证规则 1，用来放行 AP 上开启 Portal 服务的接口能够与 Portal 服务器通信。

```
portal free-rule 1 source interface GigabitEthernet 1/0/1 destination any
```

# 配置移动需求 Portal 参数。

```
portal device-id beijing-ac-01
portal url-param include nas-id param-name vlan
portal url-param include user-mac des-encrypt param-name wlanusermac
portal url-param include nas-ip param-name wlanacip
portal url-param include ap-mac param-name wlanapmac
portal url-param include user-url param-name wlanfirsturl
```

```
portal url-param include user-ip param-name wlanuserip
portal url-param include ac-name param-name wlanacname
portal url-param include ssid
```

# 创建 VLAN 168 及其接口，并进入接口视图。

```
vlan 168
interface vlan 168
```

# 开启直接认证方式的 Portal 认证。

```
portal server pt method direct
```

# 配置接口发送 Portal 报文使用的源地址为 AC 的地址。

```
portal nas-ip ipv6 2001::1
```

# 配置通过 WLAN 获取 Portal 用户信息。

```
portal host-check wlan
```

# 配置 Portal 用户报文的控制模式为 MAC。

```
portal control-mode mac
interface GigabitEthernet 1/0/1
port link-type trunk
port trunk permit vlan all
```

#### 4.4.6 配置 Portal 服务器



说明

下面以 iMC 为例(使用 iMC 版本为: iMC PLAT 7.1 (E0303)、iMC EAD 7.1 (E0303)，说明 RADIUS server 的基本配置。

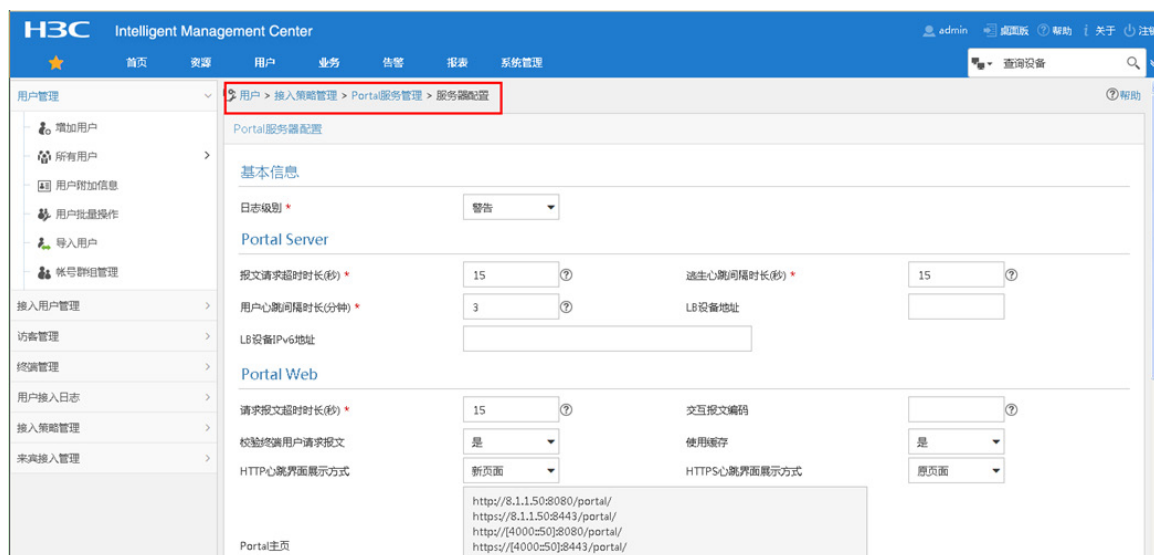
---

##### (1) 配置 Portal 服务

# 配置 Portal 服务器。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，使用缺省配置。

图13 Portal 服务器配置页面

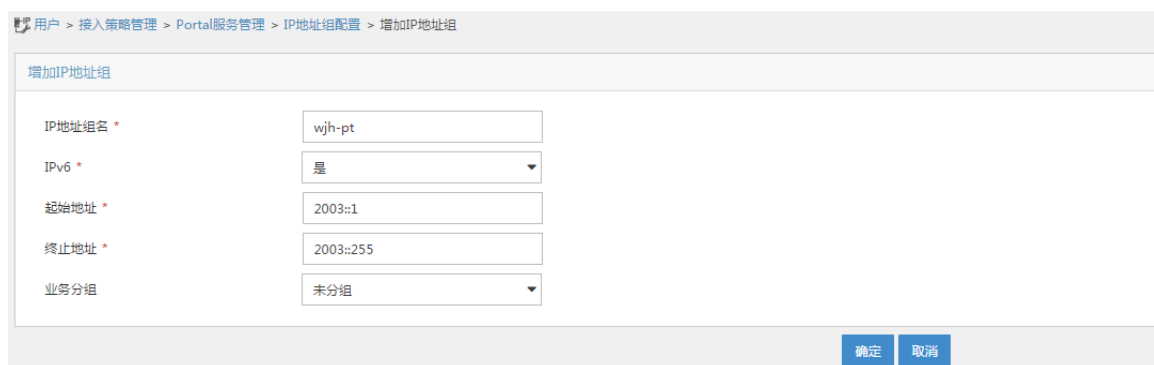


#### # 增加 Portal 地址组。

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入 IP 地址组配置页面。点击<增加>按钮，进入增加 IP 地址组页面。

- 输入 IP 地址组名：wjh-pt；
- IPv6 选择“是”；
- 输入起始地址：2003::1；
- 输入终止地址：2003::255；
- 其他采用默认配置，单击<确定>按钮完成操作。

图14 增加 IP 地址组配置页面



#### # 增加 Portal 设备。

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 输入设备名：wjh；
- 输入 IP 地址：即 AC 上配置的 portal bas-ip 地址，2001::1；
- 输入密钥：123456，与 AC 上配置的 portal server 密钥一致；
- 其他采用默认配置，单击<确定>按钮完成操作。

图15 增加设备信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

增加设备信息

设备信息

|          |            |               |         |
|----------|------------|---------------|---------|
| 设备名 *    | wjh        | 业务分组 *        | 未分组     |
| 版本 *     | Portal 3.0 | IP地址 *        | 2001::1 |
| 监听端口 *   | 2000       | 本地Challenge * | 否       |
| 认证重发次数 * | 0          | 下线重发次数 *      | 1       |
| 支持逃生心跳 * | 否          | 支持用户心跳 *      | 否       |
| 密钥 *     | *****      | 确认密钥 *        | *****   |
| 组网方式 *   | 直连         |               |         |
| 设备描述     |            |               |         |

确定 取消

# 增加端口组信息。


在 Portal 设备配置页面中的设备信息列表中，单击<端口组信息管理>按钮（“”图标），进入端口组信息配置页面。

图16 设备配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置

设备信息查询

设备名 版本 业务分组

下发结果

增加

| 设备名 | 版本         | 业务分组 | IP地址 | IPv6地址  | 最近一次下发时间 | 下发结果 | 操作                                                                                    |
|-----|------------|------|------|---------|----------|------|---------------------------------------------------------------------------------------|
| wjh | Portal 3.0 | 未分组  |      | 2001::1 |          | 未下发  |  |

共有1条记录，当前第1 - 1，第 1/1 页。

50

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 输入端口组名：w-group；
- 选择 IP 地址组：wjh-pt；
- 其他采用默认配置，单击<确定>按钮完成操作。

图17 增加端口组信息

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 增加端口组信息

帮助

增加端口组信息

端口组名 \*

w-group

开始端口 \*

0

协议类型 \*

HTTP

是否NAT \*

否

认证方式 \*

CHAP认证

心跳间隔(分钟) \*

10

用户域名

无感知认证

不支持

页面推送策略

提示语言 \*

动态检测

终止端口 \*

zzzzzz

快速认证 \*

否

错误透传 \*

是

IP地址组 \*

wjh-pt

心跳超时(分钟) \*

30

端口组描述

客户端防破解 \*

否

缺省认证页面

确定

取消

(2) 配置接入服务

# 增加接入设备。

选择“用户”标签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入到设备配置页面。在接入设备列表中单击<增加>按钮，进入增加接入设备页面。

- 选择手工增加接入设备，添加 IPv6 地址为 2001::1 的接入设备，与 AC 上 RADIUS 方案中的 nas-ip 一致；
- 设置与 AC 交互报文时使用的认证、计费共享密钥为 “123456”，该密码与 AC 配置 RADIUS 方案时的地址一致；
- 选择接入设备类型为 “H3C(General)”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图18 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \*

1812

计费端口 \*

1813

组网方式

不启用混合组网

业务类型

LAN接入业务

接入设备类型

H3C(General)

业务分组

未分组

共享密钥 \*

\*\*\*\*\*

确认共享密钥 \*

\*\*\*\*\*

接入设备分组

无

设备列表

选择

手工增加

增加IPv6设备

全部清除

| 设备名称 | 设备IP地址                                  | 设备型号 | 备注 | 删除 |
|------|-----------------------------------------|------|----|----|
|      | 2001:0000:0000:0000:0000:0000:0000:0001 |      |    |    |

共有1条记录。

确定

取消

# 增加接入策略。

选择“用户”标签，单击导航树[接入策略管理/接入策略管理]菜单项，进入到接入策略配置页面。  
在接入策略列表中点击<增加>按钮。

- 接入策略名输入“wjh-portal”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图19 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 \* wjh-portal

业务分组 \* 未分组

描述

授权信息

接入时段 无 分配IP地址 \* 否

下行速率(Kbps)

上行速率(Kbps)

优先级

启用RSA认证

证书认证 ☒ 不启用 ☐ EAP证书认证 ☐ WAPI证书认证

认证证书类型 EAP-TLS认证

下发VLAN

下发User Profile

下发ACL

下发用户组

认证绑定信息

☐ 绑定接入设备IP ☐ 绑定接入设备端口 ☐ 绑定VLAN ☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址 ☐ 绑定用户MAC地址 ☐ 绑定IMSI号码 ☐ 绑定计算机名称

☐ 计算机绑定域 ☐ 用户必须登录到域 ☐ 绑定无线SSID ☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制 ☐ 启用终端硬盘序列号控制 ☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端 ☐ 禁用Windows可溶解客户端 ☐ 禁用Linux/MacOS可溶解客户端 ☐ 禁止在线修改IP地址

☐ 网络故障时自动重连 自动重连间隔(分钟) 30 自动重连次数 3

客户端最低版本 1.00-0120

违规处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务器 ☐ 禁止IE设置代理 ☐ 禁用多网卡 ☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址 ☐ 禁止修改MAC地址 ☐ 禁止出现相同的MAC地址 ☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务 ☐ 禁止在虚拟机中运行

IP地址获取方式 ☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定 取消

# 增加接入服务。

选择“用户”标签，单击导航树[接入策略管理/接入服务管理]菜单项，进入到接入服务配置页面。  
在接入服务列表中点击<增加>按钮，进入增加接入服务页面。

- 服务名输入“wjh-portal”；
- 缺省接入策略“wjh-portal”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图20 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 \*

wjh-portal

业务分组 \*

未分组

服务后缀

缺省接入策略 \*

wjh-portal

缺省私有属性下发策略 \*

不使用

缺省单帐号最大绑定终端数 \*

0

缺省单帐号在线数量限制 \*

0

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | 优先级 | 修改 | 删除 |
|-------------|------|----------|-----|----|----|
| 未找到符合条件的记录。 |      |          |     |    |    |

确定

取消

(3) 增加接入用户。

选择“用户”标签，单击导航树中的[接入用户管理/接入用户]菜单项，进入到接入用户配置页面。在接入用户列表中点击<增加>按钮，进入增加接入用户页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“wjh-portal”；
- 输入证件号码“111111”；
- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图21 增加用户

增加用户

基本信息

用户姓名 \*

wjh-portal

✓

证件号码 \*

111111

✓

通讯地址

电话

?

电子邮件

?

用户分组 \*

未分组

检查是否可用

确定

取消

- 勾选接入服务“wjh-portal”；
- 单击<确定>按钮完成操作。



图22 增加接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

wjh-portal

选择

增加用户

帐号名 \*

wjh-portal

☐ 预开户用户

☐ 缺省BYOD用户

☐ MAC地址认证用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                            | 服务后缀 | 状态  | 分配IP地址 |
|------------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> wjh-portal |      | 可申请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

无线SSID

VLAN ID/内层VLAN ID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

MAC地址

IP地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

4.4.7 验证配置

无线客户端使用 SSID 为 portal-local 的无线服务模板上线。在浏览器输入 Portal 服务器网段的任一地址，弹出 Portal 认证页面，输入 Portal 服务器上设置的用户名和密码进行认证上线。

31

图23 用户上线

欢迎使用iMC Portal

H3C

用户名: wjh-portal

密码: .....

服务类型: [v]

☒ 保存密码

上线 下线

• [常见问题解答](#)

# 当 Portal 用户认证成功并上线之后，AC 会将用户规则下发到 AP 设备上，用户报文在 AP 上直接做转发。在 AC 上通过命令 **display portal user interface** 查看 Portal 用户成功上线。

```
<AC> display portal user interface Vlan-interface 168
```

```
Index:9
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode:stand-alone
```

```
MAC IP Vlan Interface
```

```
-----
```

| MAC            | IP      | Vlan | Interface         |
|----------------|---------|------|-------------------|
| 0021-631e-7911 | 2003::4 | 168  | Vlan-interface168 |

```
On interface Vlan-interface168:total 1 user(s) matched, 1 listed.
```

# 在 AP 上通过命令 **dis portal acl dynamic interface** 查看用户规则下发成功。

```
<ap1> display portal acl dynamic interface Vlan-interface ?
```

```
<1,168> VLAN interface
```

```
<ap1> display portal acl dynamic interface Vlan-interface 168
```

```
IPv4 portal ACL rules on Vlan-interface168:
```

```
Rule 0
```

```
Inbound interface : all
```

```
Type : dynamic
```

```
Action : permit
```

```
Source:
```

```
IP :
```

```
MAC : 0021-631e-7911
```

```
Interface : any
```

```
VLAN : 168
```

```
Protocol : 0
```

```
Destination:
```

```
IP :
```

```
Author ACL:
```

```
Number : NONE
```

#### 4.4.8 配置文件

- SwitchA

```
#
vlan 10
#
vlan 138
#
interface Bridge-Aggregation4
    port link-type trunk
    port trunk permit vlan all
#
interface Vlan-interface10
    ipv6 address 2001::50 64
#
interface Vlan-interface138
    ipv6 address 4000::1 64
#
interface Ten-GigabitEthernet4/0/1
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan all
    port link-aggregation group 4
#
interface Ten-GigabitEthernet4/0/2
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan all
    port link-aggregation group 4
#
    Ipv6 route-static 4000:: 64 4000::2
#
```

- AC

```
#
    portal server pt ipv6 4000::50 key cipher $c$3$rNRhle2UN3+u8va/OYD8LNQIHpTspvL5
ng== url http://[4000::50]:8080/portal server-type imc
    portal free-rule 1 source interface Bridge-Aggregation1 destination any
    portal host-check wlan
#
vlan 10
#
vlan 168
#
radius scheme portal
    primary authentication ipv6 4000::0050
    primary accounting ipv6 4000::0050
    key authentication cipher $c$3$M3465DvHOI26Az+zawNZzuig0Nbyao4mJg==
    key accounting cipher $c$3$9dX0xsAmXke7pEK0DpfA1wlcbEcKrjYxVQ==
```

```

user-name-format without-domain
nas-ip ipv6 2001::0001
#
domain portal
authentication portal radius-scheme portal
authorization portal radius-scheme portal
accounting portal radius-scheme portal
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 clear
ssid portal-local
bind WLAN-ESS 1
client forwarding-mode local
service-template enable
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan all
#
interface Vlan-interface10
ipv6 address 2001::1 64
#
interface Vlan-interface168
ipv6 address 4000::3 64
portal server pt method direct
portal domain ipv6 portal
portal nas-ip ipv6 2001::1
portal control-mode mac
portal forwarding-mode local
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan all
port link-aggregation group 1
#
interface WLAN-ESS1
port access vlan 168
#
wlan ap ap1 model WA2620E-AGN id 1
serial-id 210235A42MB108000001

```

```

radio 1
  service-template 1
  radio enable
radio 2
#
Ipv6 route-static :: 0 2001::2
#
•   Router
#
  ipv6 dhcp server enable
#
ipv6 dhcp pool 168
  network 2003::/64
#
interface GigabitEthernet0/0
  port link-mode route
  ipv6 address 2001::3 64
#
interface GigabitEthernet0/1.100
  vlan-type dot1q vid 100
  ipv6 address 2004::3 64
  ipv6 dhcp server apply pool 100
#
interface GigabitEthernet0/1.168
  vlan-type dot1q vid 168
  ipv6 address 2003::1 64
  ipv6 dhcp server apply pool 168
#
  Ipv6 route-static 4000:: 64 2001::2
#
•   SwitchB
#
vlan 100
#
vlan 168
#
interface Vlan-interface100
  ipv6 address 2001::3 64
#
interface Vlan-interface168
  ipv6 address 2004::2 64
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan all
#
interface GigabitEthernet1/0/2
  port link-type trunk

```

```
port trunk permit vlan all
port trunk pvid vlan 100
poe enable
#
Ipv6 route-static :: 0 2004::3
#
```

## 5 相关资料

- 《H3C WX 系列无线控制器产品配置指导》“二层技术配置指导”。
- 《H3C WX 系列无线控制器产品命令参考》“二层技术命令参考”。
- 《H3C WX 系列无线控制器产品配置指导》“WLAN 配置指导”。
- 《H3C WX 系列无线控制器产品命令参考》“WLAN 命令参考”。
- 《H3C WX 系列无线控制器产品配置指导》“安全配置指导”。
- 《H3C WX 系列无线控制器产品命令参考》“安全命令参考”。

# 基于 IPv6 的 Portal 接入认证控制功能典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                          |    |
|--------------------------|----|
| 1 简介.....                | 1  |
| 2 配置前提 .....             | 1  |
| 3 配置举例 .....             | 1  |
| 3.1 组网需求 .....           | 1  |
| 3.2 配置注意事项.....          | 2  |
| 3.3 配置步骤.....            | 2  |
| 3.3.1 AC 的配置 .....       | 2  |
| 3.3.2 Switch 的配置 .....   | 5  |
| 3.3.3 RADIUS 服务器的配置..... | 5  |
| 3.3.4 Portal 服务器的配置..... | 11 |
| 3.4 验证配置 .....           | 13 |
| 3.5 配置文件 .....           | 14 |
| 4 相关资料 .....             | 16 |



# 1 简介

本文介绍了无线控制器基于 IPv6 的 Portal 接入认证控制功能的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IPv6 Portal 的特性。

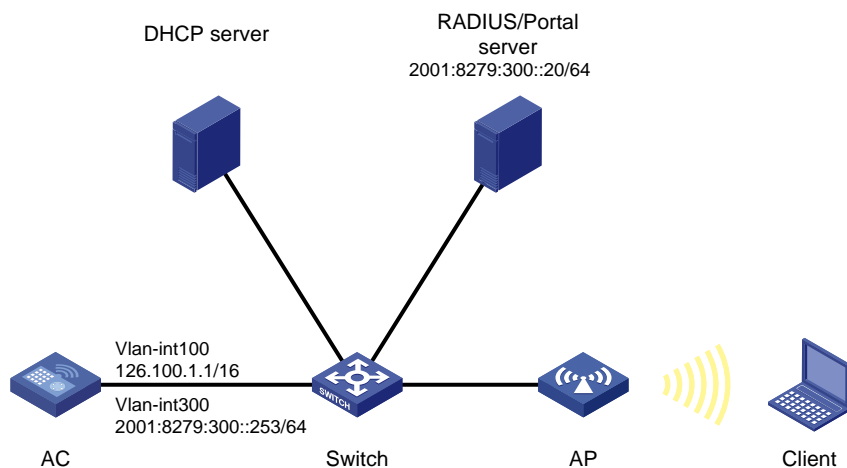
## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 通过 Switch 与 AP 相连，DHCP 服务器为 AP 分配 IPv4 地址，为 Client 分配 IPv6 地址。Client 接入到无线网络中，使用 Portal 服务器对 Client 进行基于 IPv6 的 Portal 认证。现要求：

- Client 通过 Portal 认证前，只能访问 Portal 服务器；在通过 Portal 认证后，可以使用此 IPv6 地址访问非受限的互联网资源。
- 采用 RADIUS 服务器作为认证/计费服务器。

图1 基于 IPv6 的 Portal 接入认证控制功能组网图



## 3.2 配置注意事项

- 在 AC 接口上配置的 IPv6 地址需要与 Portal 认证服务器和 RADIUS 服务器上的接入设备的 IPv6 地址保持一致。
- 保证 Client 在 Portal 认证使用的 IPv6 地址符合 Portal 服务器配置的 IPv6 地址组接入范围。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应, AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 接口

# 全局使能 IPv6 功能。

```
<AC> system-view
```

```
[AC] ipv6
```

# 创建 VLAN 100 及其对应的 VLAN 接口, 并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
[AC] vlan 100
```

```
[AC-vlan100] quit
```

```
[AC] interface vlan-interface 100
```

```
[AC-Vlan-interface100] ip address 126.100.1.1 16
```

# 取消对 RA 消息发布的抑制。

```
[AC-Vlan-interface100] undo ipv6 nd ra halt
```

# 设置被管理地址配置标志位为 1。

```
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

# 设置其他配置标志位为 1。

```
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
```

```
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
```

```
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN, 配置 VLAN 300 的接口 IPv6 地址。

```
[AC] vlan 300
```

```
[AC-vlan300] quit
```

```
[AC] interface vlan-interface 300
```

```
[AC-Vlan-interface300] ipv6 address 2001:8279:300::253 64
```

# 取消对 RA 消息发布的抑制。

```
[AC-Vlan-interface300] undo ipv6 nd ra halt
```

# 设置被管理地址配置标志位为 1。

```
[AC-Vlan-interface300] ipv6 nd autoconfig managed-address-flag
```

# 设置其他配置标志位为 1。

```
[AC-Vlan-interface300] ipv6 nd autoconfig other-flag
```

```
[AC-Vlan-interface300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS1 接口，并进入该视图。

```
[AC] interface wlan-ess 1
```

# 设置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 设置端口允许 VLAN 200 的报文不带 VLAN tag 通过。

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 设置端口禁止 VLAN 1 的报文通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

# 指定端口缺省 VLAN 为 VLAN 200。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能端口的 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

## (2) 配置 RADIUS 方案

# 创建名字为 office 的 RADIUS 方案并进入该方案视图。

```
[AC] radius scheme office
```

# 配置 RADIUS 方案的主认证服务器 IPv6 地址。

```
[AC-radius-office] primary authentication ipv6 2001:8279:300::20
```

# 配置 RADIUS 方案的主计费服务器 IPv6 地址。

```
[AC-radius-office] primary accounting ipv6 2001:8279:300::20
```

# 将 RADIUS 方案 office 的认证报文的共享密钥设置为明文 1234。

```
[AC-radius-office] key authentication simple 1234
```

# 将 RADIUS 方案 office 的计费报文的共享密钥设置为明文 1234。

```
[AC-radius-office] key accounting simple 1234
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC-radius-office] user-name-format without-domain
```

# 设置设备发送 RADIUS 报文使用的源 IP 地址为 126.100.1.1。

```
[AC-radius-rs1] nas-ip 126.100.1.1
```

```
[AC-radius-office] quit
```

## (3) 配置认证域

# 创建 office 域并进入其视图。

```
[AC] domain office
```

# 为 Portal 用户配置认证方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] authentication portal radius-scheme office
```

# 为 Portal 用户配置授权方案为 RADIUS 方案，方案名为 office。

```

[AC-isp-office] authorization portal radius-scheme office
# 为 Portal 用户配置计费方案为 RADIUS 方案，方案名为 office。
[AC-isp-office] accounting portal radius-scheme office
[AC-isp-office] quit
# 把配置的认证域 office 设置为系统缺省的 ISP 域。
[AC] domain default enable office
(4) 配置无线服务
# 创建 clear 类型的服务模板 1。
[AC] wlan service-template 1 clear
# 设置服务模板 1 的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(5) 在 AC 下绑定无线服务模板
# 创建型号为 WA2620E-AGN 的 AP 模板名为 officeap，指定其序列号。
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 配置的服务模板 1 与射频 2 关联，设置绑定到射频接口的 VLAN 编号为 VLAN 300。
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
(6) 配置 Portal 认证
# 配置 Portal 服务器 office 的 IPv6 地址为 2001:8279:300::20，密钥为 1234，URL 为
http://[2001:8279:300::20]:8080/portal。
[AC] portal server office ipv6 2001:8279:300::20 key 1234 url
http://[2001:8279:300::20]:8080/portal
# 配置 Portal 免认证规则 0，符合源接口为 GigabitEthernet1/0/1 的任意报文不会触发 Portal 认证。
[AC] portal free-rule 0 source interface gigabitethernet 1/0/1 destination any
# 配置接口 VLAN 300 使能 Portal，指定 Portal 服务器为 office，并配置为直接认证方式。
[AC] interface vlan-interface 300
[AC-Vlan-interface300] portal server office method direct
# 配置接口 VLAN 300 发送 Portal 报文使用的 IPv6 源地址为 2001:8279:300::253。
[AC-Vlan-interface300] portal nas-ip ipv6 2001:8279:300::253
# 配置接口 VLAN 300 启用 Portal 认证域 office。
[AC-Vlan-interface300] portal domain ipv6 office
# 配置 Portal 用户报文的控制模式为 MAC。
[AC-Vlan-interface300] portal control-mode mac

```

```
[AC-Vlan-interface300] quit
```

### 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300,其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量,VLAN 300 为无线客户端接入的 VLAN。

```
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk, 禁止 VLAN 1 报文通过, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 RADIUS/Portal 服务器相连的 GigabitEthernet1/0/4 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

### 3.3.3 RADIUS 服务器的配置



下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.2(E0401)、iMC UAM 5.2(E0402)），说明 RADIUS 服务器的基本配置。

---

# 启用 IPv6 功能。



- 设置认证及计费的端口号分别为“1812”和“1813”；
- 设置与 AC 交互报文时使用的认证、计费共享密钥为“1234”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 选择“增加 IPv6 设备”，添加 IPv6 地址为“2001:8279:300::253”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 增加接入设备

业务 >> 用户接入管理 >> 接入设备管理 >> 接入设备配置 >> 增加接入设备

帮助

接入配置

\* 认证端口

1812

\* 计费端口

1813

\* 共享密钥

●●●●

\* 确认共享密钥

●●●●

接入区域

无

业务类型

LAN接入业务

接入设备类型

H3C(General)

组网方式

不启用混合组网

业务分组

未分组

设备列表

选择

手工增加

增加IPv6设备

全部清除

共有1条记录。

| 设备名称 | 设备IP地址                             | 设备型号 | 备注 | 删除 |
|------|------------------------------------|------|----|----|
|      | 2001:8279:0300:0000:0000:0000:0253 |      |    | ✖  |

确定

取消

# 配置接入规则。

选择“业务”页签，单击导航树中的[用户接入管理/接入规则管理]菜单项，单击<增加>按钮，创建一条接入规则。

- 接入规则名输入“office”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 配置接入规则

业务 >> 用户接入管理 >> 接入规则管理 >> 增加接入规则

帮助

基本信息

接入规则名

office

业务分组

未分组

描述

授权信息

接入时段

无

分配IP地址

否

下行速率

Kbps

上行速率

Kbps

优先级

☐ 启用RSA认证

证书认证

☒ 不启用 ☐ EAP证书认证 ☐ WAPI证书认证

认证证书类型

EAP-TLS认证

下发VLAN

☐ 下发User Profile

下发用户组

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线用户SSID

☐ 绑定接入设备序列号

☐ 启用接入MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线用户SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Windows可溶解客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔

30

自动重连次数

3

违规处理模式

☐ 下线 ☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

IP地址获取方式

☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定

取消

# 增加服务配置。

选择“业务”页签，单击导航树中的[用户接入管理/服务配置管理]菜单项，进入服务器配置管理页面，在该页面中单击<增加>按钮，进入增加服务配置页面。

- 输入服务名为“office”、服务后缀为“office”；
- 缺省接入规则输入“office”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。



图5 增加服务配置

 业务 >> 用户接入管理 >> 服务配置管理 >> 增加服务配置

 帮助

基本信息

\* 服务名

office

服务后缀

office

\* 业务分组

未分组

\* 缺省接入规则

office

\* 缺省私有属性下发策略

不使用

计费策略

不计费

服务描述

☒ 可申请

☐ Portal智能终端快速认证

接入策略列表

增加

| 接入场景 | 接入规则 | 私有属性下发策略 | 优先级 | 修改 | 删除 |
|------|------|----------|-----|----|----|
|------|------|----------|-----|----|----|

确定

取消

- # 增加用户配置。
- 选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户]菜单项，单击<增加>按钮，增加一个接入用户，再选择<增加用户>。
- 用户姓名输入“portaluser”；
  - 证件号码输入“1234”；
  - 用户分组选择“未分组”；
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加用户配置

增加用户

基本信息

\* 用户姓名

portaluser

\* 证件号码

1234

通讯地址

电话

电子邮件

\* 用户分组

未分组

确定

取消

- # 增加接入用户配置。
- 返回主页面，输入：
- 账号名输入“office”；
  - 密码与密码确认输入“1234”；
  - 选择服务名“office”；
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。

图7 增加接入用户配置

 用户 >> 所有接入用户 >> 增加接入用户

 帮助

接入用户

接入信息

\* 用户姓名

portaluser

选择

增加用户

\* 帐号名

office

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

\* 密码

....

\* 密码确认

....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

失效日期

Porta智能终端最大绑定数

1

最大闲置时长

分钟

在线数量限制

1

帐号类型

预付费

\* 预付金额

0

元

自助充值

允许

登录提示信息

接入服务

|                                     | 服务名    | 服务后缀   | 状态  | 计费策略 | 分配IP地址 |
|-------------------------------------|--------|--------|-----|------|--------|
| <input checked="" type="checkbox"/> | office | office | 可申请 | User |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

无线用户SSID

VLAN ID/内层VLAN ID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

绑定域

MAC地址

IP地址

 提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

### 3.3.4 Portal 服务器的配置



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.2(E0401)、iMC UAM 5.2(E0402)），说明 Portal 服务器的基本配置。

# 配置 Portal 服务器。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[用户接入管理/Portal 服务器管理/服务器配置]菜单项，进入服务器配置页面。

- Portal 主页选择 `http://2001:8279:300::20:8080/portal/`;
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8 Portal 认证服务器配置页面

业务 >> 用户接入管理 >> Portal 服务器管理 >> 服务器配置 帮助

Portal 服务器配置

基本信息

\* 日志级别

信息

\* 报文请求超时时长

4

秒

\* 逃生心跳间隔时长

20

秒

\* 用户心跳间隔时长

5

分

钟

Portal 主页

`http://2001:8279:300::20:8080/portal/`

高级信息

服务类型列表

增加

共有0条记录。

| 服务类型标识 | 服务类型 | 删除 |
|--------|------|----|
|--------|------|----|

确定

# 配置 IPv6 地址组。

单击导航树中的[用户接入管理/Portal 服务管理/IP 地址组配置]菜单项，进入 IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名 “portaluser”；
- 输入起始地址 “2001:8279:300::0”；
- 输入终止地址 “2001:8279:300::FFFF:FFFF:FFFF:FFFF”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9 增加 IP 地址组配置页面

业务 >> 用户接入管理 >> Portal服务管理 >> IP地址组配置 >> 增加IP地址组 帮助

---

**增加IP地址组**

\* IP地址组名

\* IPv6

\* 起始地址

\* 终止地址

业务分组

# 配置 Portal 设备。

单击导航树中的[用户接入管理/Portal 服务管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名 “NAS”；
- 指定 IP 地址为与接入用户相连的设备接口 IPv6 地址 “2001:8279:300::253”；
- 选择版本，Portal 3.0；
- 密钥与密钥确认输入 “1234” 与 AC 上的配置保持一致；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图10 增加设备信息配置页面

业务 >> 用户接入管理 >> Portal服务管理 >> 设备配置 >> 增加设备信息 帮助

---

**增加设备信息**

**设备信息**

|                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>* 设备名 <input type="text" value="NAS"/></p> <p>* 版本 <input type="text" value="Portal 3.0"/></p> <p>* 监听端口 <input type="text" value="2000"/></p> <p>* 认证重发次数 <input type="text" value="0"/></p> <p>* 支持逃生心跳 <input type="text" value="否"/></p> <p>* 密钥 <input type="text" value="...."/></p> <p>* 组网方式 <input type="text" value="三层"/></p> <p>设备描述 <input type="text"/></p> | <p>* 业务分组 <input type="text" value="未分组"/></p> <p>* IP地址 <input type="text" value="2001:8279:300::253"/></p> <p>* 本地Challenge <input type="text" value="否"/></p> <p>* 下线重发次数 <input type="text" value="1"/></p> <p>* 支持用户心跳 <input type="text" value="否"/></p> <p>* 确认密钥 <input type="text" value="...."/></p> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

# Portal 设备关联 IPv6 地址组

在 Portal 设备配置页面中的设备信息列表中，点击 NAS 设备的<操作|端口组信息管理>链接，进入端口组信息配置页面。

图11 设备信息列表

业务 >> 用户接入管理 >> Portal服务管理 >> 设备配置

加入收藏 帮助

增加设备“NAS”成功。

设备信息查询

设备名  版本

下发结果  业务分组

查询 重置

设备信息列表

增加

共有1条记录，当前第1 - 1，第 1/1 页。 每页显示: 8 15 [50] 100 200

| 设备名 | 版本         | 业务分组 | IP地址 | IPv6地址             | 最近一次下发时间 | 下发结果 | 操作                                                             |
|-----|------------|------|------|--------------------|----------|------|----------------------------------------------------------------|
| NAS | Portal 3.0 | 未分组  |      | 2001:8279:300::253 |          |      | <div>修改</div> <div>删除</div> <div>端口组信息管理</div> <div>下发配置</div> |

# 配置端口组信息。

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名“group”；
- 选择IP地址组“portaluser”，用户接入网络时使用的IP地址必须属于所选的IP地址组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图12 增加端口组信息配置页面

业务 >> 用户接入管理 >> Portal服务管理 >> 设备配置 >> 端口组信息配置 >> 增加端口组信息

帮助

增加端口组信息

\* 端口组名

group

\* 开始端口

0

\* 协议类型

HTTP

\* 是否NAT

否

\* 认证方式

CHAP认证

\* 心跳间隔

10

分钟

用户域名

智能终端快速认证

不支持

用户属性类型

缺省认证页面

index\_default.jsp

\* 提示语言

动态检测

\* 终止端口

zzzzzz

\* 快速认证

否

\* 错误透传

是

\* IP地址组

portaluser

\* 心跳超时

30

分钟

端口组描述

\* 客户端防破解

否

缺省认证类型

网页身份认证

确定

取消

3.4 验证配置

# 使用命令 `display wlan ap all` 可以看到 AP 与 AC 已经成功建立连接。

```
<AC> display wlan ap all
Total Number of APs configured          : 1
Total Number of configured APs connected : 1
Total Number of auto APs connected      : 0

AP Profiles
State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
       C = Config, R = Run, KU = KeyUpdate, KC = KeyCfm
       M = Master, B = Backup
```

| AP Name  | State Model     | Serial-ID           |
|----------|-----------------|---------------------|
| officeap | R/M WA2620E-AGN | 21023529G007C000020 |

# 通过 **display wlan client** 命令可以看到 Client 通过 SSID service 使用 VLAN 300 成功接入，此时 Client 只能够 ping 通 Portal server 的地址。

```
<AC> display wlan client
Total Number of Clients          : 1

Client Information
```

| MAC Address    | User Name | APID/RID | IP Address | VLAN |
|----------------|-----------|----------|------------|------|
| 0024-d77d-52bc | -NA-      | 1 /2     | 0.0.0.0    | 300  |

# Client 通过访问 HTTP 的 IPv6 地址触发 Portal 认证，输入正确的用户名 office 和密码 1234 后，能够认证成功。通过 Portal 认证后，可以访问网络资源。

```
<AC> display portal user all
Index:0
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC          IP          Vlan    Interface
-----
0024-d77d-52bc  2001:8279:300:0:1  300    Vlan-interface300
Total 1 user(s) matched, 1 listed.
```

## 3.5 配置文件

- AC:
 

```
#
domain default enable office
#
ipv6
#
portal server office ipv6 2001:8279:300::20 key cipher
$c$3$RlNc0UcQcm1IEkYVmswceR2faejx77o= url http://[2001:8279:300::20]:8080/portal
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
```

```

#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
    primary authentication ipv6 2001:8279:300::20
    primary accounting ipv6 2001:8279:300::20
    key authentication cipher $c$3$LAeobkoqSbPOxIzI4RZav+igpYNsn4M=
    key accounting cipher $c$3$LAeobkoqSbPOxIzI4RZav+igpYNsn4M=
    user-name-format without-domain
    nas-ip 126.100.1.1
#
domain office
    authentication portal radius-scheme office
    authorization portal radius-scheme office
    accounting portal radius-scheme office
    access-limit disable
    state active
    idle-cut disable
    self-service-url disable
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
interface Vlan-interface100
    ip address 126.100.1.1 255.255.0.0
#
interface Vlan-interface300
    ipv6 address 2001:8279:300::253/64
    portal control-mode mac
    portal server office method direct
    portal nas-ip ipv6 2001:8279:300::253
    portal domain ipv6 office
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 300
    undo port trunk permit vlan 1
    port trunk pvid vlan 100
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1

```

```

port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
  service-template 1 vlan-id 300
  radio enable
#

```

#### ● Switch:

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 300
  undo port trunk permit vlan 1
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 100
#
interface GigabitEthernet1/0/4
  port link-type access
  port access vlan 100
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。



# 基于 SSID 绑定 Portal 服务器和认证服务器典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                          |    |
|--------------------------|----|
| 1 简介.....                | 1  |
| 2 配置前提 .....             | 1  |
| 3 配置举例 .....             | 1  |
| 3.1 组网需求 .....           | 1  |
| 3.2 配置思路 .....           | 2  |
| 3.3 配置注意事项 .....         | 2  |
| 3.4 配置步骤 .....           | 2  |
| 3.4.1 AC 的配置 .....       | 2  |
| 3.4.2 Switch 的配置 .....   | 5  |
| 3.4.3 RADIUS 服务器配置 ..... | 6  |
| 3.5 验证配置 .....           | 10 |
| 3.6 配置文件 .....           | 12 |
| 4 相关资料 .....             | 14 |

# 1 简介

本文档介绍 Portal 服务器绑定两个 SSID，并对通过这两个 SSID 上线的用户进行认证的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 Portal、AAA 和 WLAN 特性。

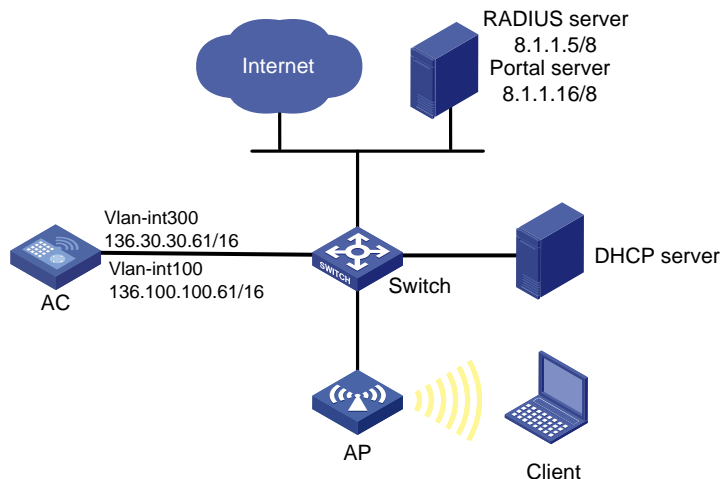
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，Client 和 AP 通过 DHCP 服务器获取 IP 地址，Client 需要通过指定的 SSID 访问特定的 Portal 服务器。具体要求如下：

- 当 Client 通过名称为 service1 的 SSID 上线时，只能在名称为 office1 的 Portal 服务器上进行 Portal 认证。
- 当 Client 通过名称为 service2 的 SSID 上线时，只能在名称为 office2 的 Portal 服务器上进行 Portal 认证。
- Client 在通过 Portal 认证前，只能访问 Portal 服务器；在通过 Portal 认证后，可以访问非受限互联网资源。

图1 配置 Portal 认证组网图



## 3.2 配置思路

- 为了使 Client 在不同的 Portal 服务器上认证，需要配置两个 Portal 服务器和两个认证域。
- 为了使 Client 从不同的 SSID 上线时访问不同的 Portal 服务器，需要将指定的 SSID 与指定的 Portal 服务器及认证域绑定。

## 3.3 配置注意事项

- AC 上配置的密钥和 Portal 服务器上配置的密钥需要保持一致。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 136.100.100.61 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并配置其接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 136.30.30.61 255.255.0.0
[AC-Vlan-interface300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置无线接口

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置 WLAN-ESS1 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```

[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
# 使能 MAC-VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
# 创建 WLAN-ESS2 接口，并设置端口的链路类型为 Hybrid 类型。
[AC] interface wlan-ess 2
[AC-WLAN-ESS2] port link-type hybrid
# 配置 WLAN-ESS2 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC-WLAN-ESS2] undo port hybrid vlan 1
[AC-WLAN-ESS2] port hybrid pvid vlan 200
[AC-WLAN-ESS2] port hybrid vlan 200 untagged
# 使能 MAC-VLAN 功能。
[AC-WLAN-ESS2] mac-vlan enable
[AC-WLAN-ESS2] quit
(3) 配置无线服务
# 创建 clear 类型的服务模板 1。
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service1。
[AC-wlan-st-1] ssid service1
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
# 创建 clear 类型的服务模板 2。
[AC] wlan service-template 2 clear
# 设置当前服务模板的 SSID 为 service2。
[AC-wlan-st-2] ssid service2
# 将 WLAN-ESS2 接口绑定到服务模板 2。
[AC-wlan-st-2] bind wlan-ess 2
# 启用无线服务。
[AC-wlan-st-2] service-template enable
[AC-wlan-st-2] quit
# 创建 AP 的管理模板，名称为 officeap1，型号名称选择 WA2620E-AGN，并配置 AP 的序列号。
[AC] wlan ap officeap1 model WA2620E-AGN
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap1] radio 2
# 将服务模板绑定到 Radio 口。
[AC-wlan-ap-officeap1-radio-2] service-template 1 vlan-id 300
[AC-wlan-ap-officeap1-radio-2] service-template 2 vlan-id 300
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap1-radio-2] radio enable

```

```
[AC-wlan-ap-officeap1-radio-2] quit
```

```
[AC-wlan-ap-officeap1] quit
```

#### (4) 配置 AAA 认证

# 创建 RADIUS 方案 office1 并进入其视图。

```
[AC] radius scheme office1
```

# 配置 RADIUS 服务器类型为 extended。

```
[AC-radius-office1] server-type extended
```

# 配置主认证与主计费 RADIUS 服务器的 IP 地址 8.1.1.5。

```
[AC-radius-office1] primary authentication 8.1.1.5
```

```
[AC-radius-office1] primary accounting 8.1.1.5
```

# 配置系统与认证和计费 RADIUS 服务器交互报文时的共享密钥为 office。

```
[AC-radius-office1] key authentication office
```

```
[AC-radius-office1] key accounting office
```

# 指定发送给 RADIUS 方案 office1 中 RADIUS 服务器的用户名不得携带域名。

```
[AC-radius-office1] user-name-format without-domain
```

# 指定设备发送 Radius 报文使用的源地址为 136.100.100.61，Radius 服务器上配置的接入设备的地址必须与该地址相同。（若不指定源地址，设备将以发送 Radius 报文的出接口的地址作为源地址，此时请确保 Radius 服务器上配置的接入设备的地址与该出接口地址相同）

```
[AC-radius-office1] nas-ip 136.100.100.61
```

```
[AC-radius-office1] quit
```

# 创建 office1 域并进入其视图。

```
[AC] domain office1
```

# 为 Portal 用户配置认证方案为 RADIUS 方案，方案名为 office1。

```
[AC-isp-office1] authentication portal radius-scheme office1
```

# 为 Portal 用户配置授权方案为 RADIUS 方案，方案名为 office1。

```
[AC-isp-office1] authorization portal radius-scheme office1
```

# 为 Portal 用户配置计费方案为 RADIUS 方案，方案名为 office1。

```
[AC-isp-office1] accounting portal radius-scheme office1
```

```
[AC-isp-office1] quit
```

# 创建 RADIUS 方案 office2 并进入其视图。

```
[AC] radius scheme office2
```

# 配置 RADIUS 服务器类型为 extended。

```
[AC-radius-office2] server-type extended
```

# 配置主认证与主计费 RADIUS 服务器的 IP 地址 8.1.1.16。

```
[AC-radius-office2] primary authentication 8.1.1.16
```

```
[AC-radius-office2] primary accounting 8.1.1.16
```

# 配置系统与认证和计费 RADIUS 服务器交互报文时的共享密钥为 office。

```
[AC-radius-office2] key authentication office
```

```
[AC-radius-office2] key accounting office
```

# 指定发送给 RADIUS 方案 office2 中 RADIUS 服务器的用户名不得携带域名。

```
[AC-radius-office2] user-name-format without-domain
```

# 指定设备发送 Radius 报文使用的源地址为 136.100.100.61，Radius 服务器上配置的接入设备的地址必须与该地址相同。（若不指定源地址，设备将以发送 Radius 报文的出接口的地址作为源地址，此时请确保 Radius 服务器上配置的接入设备的地址与该出接口地址相同）

```

[AC-radius-office2] nas-ip 136.100.100.61
[AC-radius-office2] quit
# 创建 office2 域并进入其视图。
[AC] domain office2
# 为 Portal 用户配置认证方案为 RADIUS 方案，方案名为 office2。
[AC-isp-office2] authentication portal radius-scheme office2
# 为 Portal 用户配置授权方案为 RADIUS 方案，方案名为 office2。
[AC-isp-office2] authorization portal radius-scheme office2
# 为 Portal 用户配置计费方案为 RADIUS 方案，方案名为 office2。
[AC-isp-office2] accounting portal radius-scheme office2
[AC-isp-office2] quit
(5) 配置 Portal 认证
# 配置 Portal 服务器 office1 和 office2。
[AC] portal server office1 ip 8.1.1.5 key simple office url http://8.1.1.5:8080/portal
[AC] portal server office2 ip 8.1.1.16 key simple office url http://8.1.1.16:8080/portal
# 配置 Portal 免认证规则。
[AC] portal free-rule 1 source ip any destination ip 8.1.1.5 mask 255.255.255.255
[AC] portal free-rule 2 source ip any destination ip 8.1.1.16 mask 255.255.255.255
# 配置 service2 的 SSID 与名称为 office2 的 portal server 及名称为 office2 的认证域绑定。
[AC] portal wlan ssid service2 server office2 domain office2
# 在 VLAN 300 的接口上使能直接 Portal 认证。
[AC] interface vlan-interface 300
[AC-Vlan-interface300] portal server office1 method direct
# 指定 Portal 用户使用的认证域为 office1。
[AC-Vlan-interface300] portal domain office1
# 配置接口的 NAS-Port-Type 为符合 IEEE 802.11 标准的无线接口类型。
[AC-Vlan-interface300] portal nas-port-type wireless
# 配置接口发送 Portal 报文使用的 IPv4 源地址为 136.100.100.61。
[AC-Vlan-interface300] portal nas-ip 136.100.100.61
[AC-Vlan-interface300] quit

```

### 3.4.2 Switch 的配置

```

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN
300 为无线用户接入的 VLAN。
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
# 配置 Switch 的 GigabitEthernet1/0/1 接口的属性为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许
VLAN 100 和 VLAN 300 通过。
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300

```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

### 3.4.3 RADIUS 服务器配置



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.2(E0401)、iMC UAM 5.2(E0401)），说明 RADIUS 服务器的基本配置。

# 增加接入设备。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[用户接入管理/接入设备管理/接入设备配置]菜单项，单击<增加>按钮，进入“增加接入设备”页面，单击<手工增加>按钮，进入“手工增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“office”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 136.100.100.61 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备



# 配置接入规则。

选择“业务”页签，单击导航树中的[用户接入管理/接入规则管理]菜单项，单击<增加>按钮，创建一条接入规则。

- 接入规则名输入“portal”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 配置接入规则

业务 >> 用户接入管理 >> 接入规则管理 >> 增加接入规则

|                                         |                                                                                                   |                                  |   |
|-----------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------|---|
| <b>基本信息</b>                             |                                                                                                   |                                  |   |
| * 接入规则名                                 | portal                                                                                            |                                  |   |
| * 业务分组                                  | 未分组                                                                                               |                                  |   |
| 描述                                      |                                                                                                   |                                  |   |
| <b>授权信息</b>                             |                                                                                                   |                                  |   |
| 接入时段                                    | 无                                                                                                 | * 分配IP地址                         | 否 |
| 下行速率                                    |                                                                                                   | 上行速率                             |   |
| 优先级                                     |                                                                                                   | <input type="checkbox"/> 启用RSA认证 |   |
| 证书认证                                    | <input checked="" type="radio"/> 不启用 <input type="radio"/> EAP证书认证 <input type="radio"/> WAPI证书认证 |                                  |   |
| 认证证书类型                                  | EAP-TLS认证                                                                                         |                                  |   |
| 下发VLAN                                  |                                                                                                   |                                  |   |
| <input type="checkbox"/> 下发User Profile |                                                                                                   | 下发用户组                            |   |
| <input type="checkbox"/> 下发ACL          |                                                                                                   |                                  |   |

# 增加接入服务配置。

选择“业务”页签，单击导航树中的[用户接入管理/服务配置管理]菜单项，单击<增加>按钮，创建一条接入服务。

- 服务名输入“portal”。
- 缺省接入规则输入“portal”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 配置接入服务

业务 >> 用户接入管理 >> 服务配置管理 >> 增加服务配置

|                                         |                                         |          |        |
|-----------------------------------------|-----------------------------------------|----------|--------|
| <b>基本信息</b>                             |                                         |          |        |
| * 服务名                                   | portal                                  | 服务后缀     |        |
| * 业务分组                                  | 未分组                                     | * 缺省接入规则 | portal |
| * 缺省私有属性下发策略                            | 不使用                                     |          |        |
| 服务描述                                    |                                         |          |        |
| <input checked="" type="checkbox"/> 可申请 | <input type="checkbox"/> Portal智能终端快速认证 |          |        |
| <b>接入策略列表</b>                           |                                         |          |        |
| 增加                                      |                                         |          |        |
| 接入场景                                    | 接入规则                                    | 私有属性下发策略 | 优先级    |
|                                         |                                         |          | 修改     |
|                                         |                                         |          | 删除     |
| 确定 取消                                   |                                         |          |        |

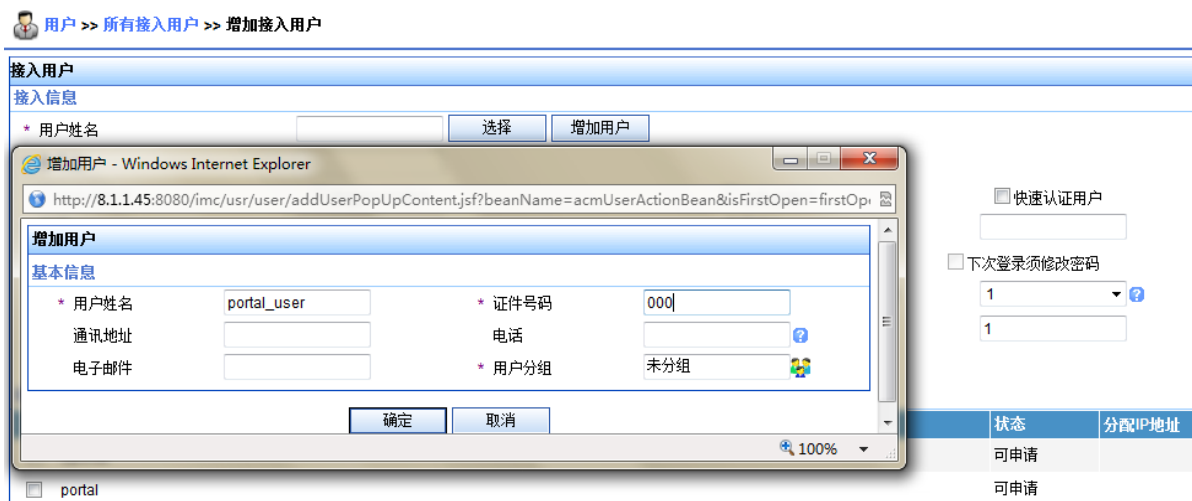
# 增加用户配置。

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户/接入用户列表]菜单项，单击<增加>按钮，增加一个接入用户。

- 单击“增加用户”。

- 用户姓名输入“portal\_user”。
- 证件号码输入“000”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 增加用户配置



#### # 增加接入用户配置。

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户/接入用户列表]菜单项，单击<增加>按钮，增加一个接入用户。

- 账号名输入“portal”。
- 密码与密码确认输入“portal”。
- 选择服务名“portal”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加接入用户配置



#### # 增加 IP 地址组配置。

选择“业务”页签，单击导航树中的[用户接入管理/Portal 服务管理/IP 地址组配置]菜单项，单击<增加>按钮，配置进行 Portal 认证的地址组范围。

- 配置 IP 地址组名为 ipgroup100。
- 配置起始地址为 136.100.0.1。
- 配置终止地址为 136.100.255.255。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图7 增加 IP 地址组

业务 >> 用户接入管理 >> Portal服务管理 >> IP地址组配置 >> 增加IP地址组

---

**增加IP地址组**

|          |                 |
|----------|-----------------|
| * IP地址组名 | ipgroup100      |
| * IPv6   | 否               |
| * 起始地址   | 136.100.0.1     |
| * 终止地址   | 136.100.255.255 |
| 业务分组     | 未分组             |
| * 类型     | 普通              |

确定 取消

# 增加 Portal 设备配置。

选择“业务”页签，单击导航树中的[用户接入管理/Portal 服务管理]菜单项，单击“设备配置”进入设备信息列表页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 设备名输入“AC”；
- IP 地址输入“136.100.100.61”；
- 密钥与密钥确认输入“office”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8 增加 Portal 设备

业务 >> 用户接入管理 >> Portal服务管理 >> 设备配置 >> 增加设备信息

---

**增加设备信息**

设备信息

|          |            |               |                |
|----------|------------|---------------|----------------|
| * 设备名    | AC         | * 业务分组        | 未分组            |
| * 版本     | Portal 2.0 | * IP地址        | 136.100.100.61 |
| * 监听端口   | 2000       | * 本地Challenge | 否              |
| * 认证重发次数 | 0          | * 下线重发次数      | 1              |
| * 支持逃生心跳 | 否          | * 支持用户心跳      | 否              |
| * 密钥     | *****      | * 确认密钥        | *****          |
| * 组网方式   | 三层         |               |                |
| 设备描述     |            |               |                |

确定 取消

# 进入 Portal 端口组。

选择“业务”页签，单击导航树中的[用户接入管理/Portal 服务管理]菜单项，单击“设备配置”进入设备信息列表页面，在该页面中单击<操作>按钮，选择<端口组信息管理>按钮，进入端口组信息列表页面。

图9 进入 Portal 端口组



# 增加 Portal 端口组配置。

进入端口组信息列表页面后，单击<增加>按钮，进入增加端口组信息配置页面。

- 端口组名输入“portgroup”；
- IP 地址组选择“ipgroup”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图10 配置 Portal 端口组信息



### 3.5 验证配置

客户端分别通过 service1 和 service2 的 SSID 上线，并进行 Portal 认证。

# 使用命令 **display portal user all** 可以查看到有用用户在线。

```
[AC] display portal user all
Index:66
```

```

State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC                IP                Vlan                Interface
-----
0015-005c-8b2c     136.30.0.1        300                Vlan-interface300
Total 1 user(s) matched, 1 listed.

```

# 通过命令 **display connection ucibindex** 可以查看到在线用户的详细信息。此时，客户端接入 SSID 为 **service2**，由于 **service2** 已经绑定全局 **Portal server** 和 **domain**，因此未使用 **VLAN** 接口下的 **Portal server** 和 **domain**。

```

[AC]display connection ucibindex 66
Index=66 , Username=portal@office2
MAC=00-15-00-5C-8B-2C
IP=136.30.0.1
IPv6=N/A
Access=PORTAL ,AuthMethod=CHAP
Port Type=Wireless-802.11,Port Name=Vlan-interface300
Initial VLAN=300, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
SessionTimeout=86333(s), Terminate-Action=Default
Start=2014-01-06 13:46:23 ,Current=2014-01-06 13:50:31 ,Online=00h04m08s
Total 1 connection matched.

```

# 使用命令 **display portal user all** 可以查看到有用户在线。

```

[AC] display portal user all
Index:68
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC                IP                Vlan                Interface
-----
0015-005c-8b2c     136.30.0.1        300                Vlan-interface300
Total 1 user(s) matched, 1 listed.

```

# 通过命令 **display connection ucibindex** 可以看到在线用户的详细信息。此时，客户端接入 SSID 为 **service1**，由于 **service1** 未经绑定全局 **portal server** 和 **domain**，因此使用 **VLAN** 接口下的 **Portal server** 和 **domain**

```

[AC] display connection ucibindex 68
Index=68 , Username=portal@office1
MAC=00-15-00-5C-8B-2C
IP=136.30.0.1

```

```

IPv6=N/A
Access=PORTAL ,AuthMethod=CHAP
Port Type=Wireless-802.11,Port Name=Vlan-interface300
Initial VLAN=300, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
SessionTimeout=86377(s), Terminate-Action=Default
Start=2014-01-06 14:00:17 ,Current=2014-01-06 14:00:41 ,Online=00h00m24s
Total 1 connection matched.

```

## 3.6 配置文件

- AC:

```

#
 portal server officel ip 8.1.1.5 key cipher $c$3$2NWtEIcPlCJ+BN29VR0Ux1Iiqu5Kew
 == url http://8.1.1.5:8080/portal
 portal server office2 ip 8.1.1.16 key cipher $c$3$830ONOk07BvvwCoY2NKLjbpqiUHfG
 gw== url http://8.1.1.16:8080/portal
 portal free-rule 1 source ip any destination ip 8.1.1.5 mask 255.255.255.255
 portal free-rule 2 source ip any destination ip 8.1.1.16 mask 255.255.255.255
 portal wlan ssid service2 server office2 domain office2
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme officel
 server-type extended
 primary authentication 8.1.1.5
 primary accounting 8.1.1.5
 key authentication cipher $c$3$do4lsdb353XNO8Ab8KV2/MX9i90/0g==
 key accounting cipher $c$3$1+8y/LRf8fEB6bDWPkbUk4/hz5B9sA==
 user-name-format without-domain
 nas-ip 136.100.100.61
radius scheme office2
 server-type extended
 primary authentication 8.1.1.16
 primary accounting 8.1.1.16
 key authentication cipher $c$3$2ZO010eUIsGDxt7RRICLqUUD5AxqkQ==
 key accounting cipher $c$3$7E/xAC2w1WGjUSpzlrH30/8FYVJzNg==
 user-name-format without-domain
 nas-ip 136.100.100.61
#
domain officel

```

```

authentication portal radius-scheme officel
authorization portal radius-scheme officel
accounting portal radius-scheme officel
access-limit disable
state active
idle-cut disable
self-service-url disable
domain office2
authentication portal radius-scheme office2
authorization portal radius-scheme office2
accounting portal radius-scheme office2
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 clear
ssid service1
bind WLAN-ESS 1
service-template enable
#
wlan service-template 2 clear
ssid service2
bind WLAN-ESS 2
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200 300
#
interface Vlan-interface100
ip address 136.100.100.61 255.255.0.0
#
interface Vlan-interface300
ip address 136.30.30.61 255.255.0.0
portal server officel method direct
portal domain officel
portal nas-port-type wireless
portal nas-ip 136.100.100.61
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#

```

```

interface WLAN-ESS2
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap officeap1 model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
    service-template 1 vlan-id 300
    service-template 2 vlan-id 300
  radio enable
#

```

- **Switch:**

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 100 300
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
  poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。



# 双机热备下的本地 Portal 认证典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                               |    |
|-------------------------------|----|
| 1 简介.....                     | 1  |
| 2 配置前提 .....                  | 1  |
| 3 配置举例 .....                  | 1  |
| 3.1 组网需求 .....                | 1  |
| 3.2 配置思路 .....                | 2  |
| 3.3 配置注意事项.....               | 2  |
| 3.4 配置步骤 .....                | 3  |
| 3.4.1 AC 1 的配置 .....          | 3  |
| 3.4.2 AC 2 的配置 .....          | 6  |
| 3.4.3 Switch 1 的配置 .....      | 10 |
| 3.4.4 Switch 2 的配置 .....      | 10 |
| 3.4.5 RADIUS Server 的配置 ..... | 11 |
| 3.5 验证配置 .....                | 16 |
| 3.6 配置文件 .....                | 16 |
| 4 相关资料 .....                  | 21 |

# 1 简介

本文介绍了双机热备下的本地 Portal 认证典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 无线接入、Portal 认证、双 AC 备份等特性。

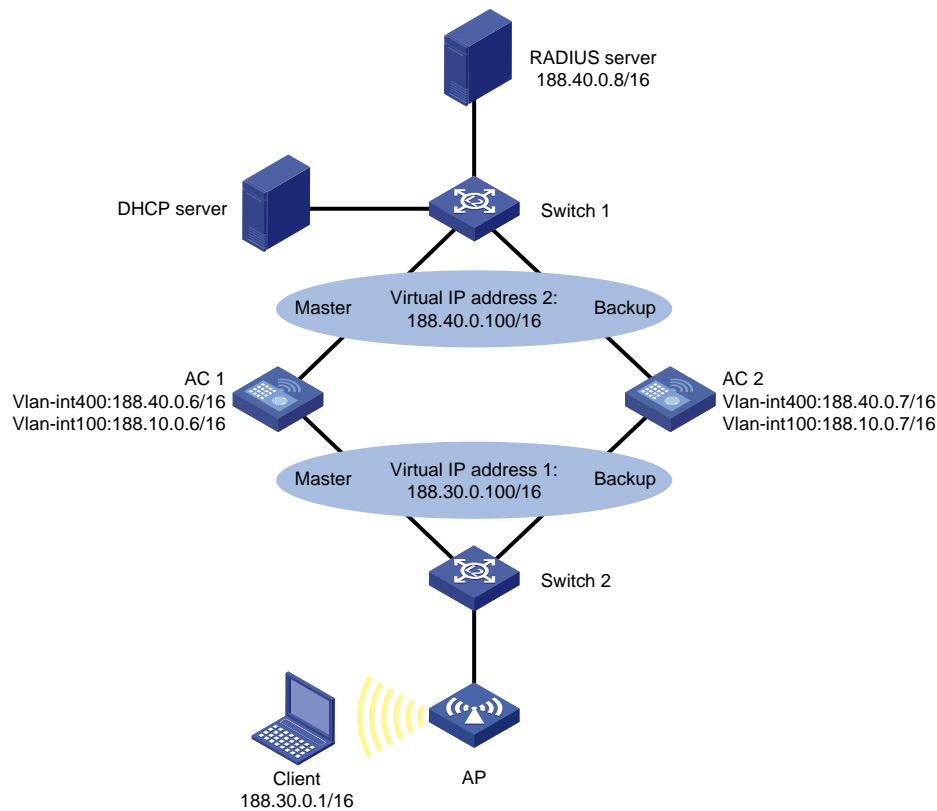
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，为了提高无线用户接入的可靠性，要求在 AC 1 和 AC 2 之间实现双机热备功能，并且对 Portal 用户的数据进行备份。具体需求如下：

- AC1 和 AC2 通过 VLAN 10 传输双机热备报文。
- AC 1 正常工作的情况下，Client 通过 AC 1 进行 Portal 认证接入到外网。AC 1 发生故障的情况下，Client 通过 AC 2 接入到外网，保证业务流量切换不被中断。
- 采用 RADIUS 服务器作为认证/计费服务器，采用 AC 作为本地 Portal 服务器。
- 当 Portal 用户异常下线时，为了防止 AC 误认为异常下线用户仍在线，可以通过用户闲置切断功能来实现。

图1 双机热备下的本地 Portal 认证组网图



## 3.2 配置思路

- 为了避免两台 AC 和上下行设备产生环路，并在主备切换时，尽快完成收敛，需要在 AC 1 和 AC 2 上使能 MSTP 功能，并设置 AC 1 为根桥。
- 当发生主备切换时，为了保证 AC 的上下行不丢包，需要分别在 AC 1 和 AC 2 的上下行接口上配置 VRRP 备份组。
- 为了使 AC 1 成为 VRRP 备份组的 Master AC，需要在 VRRP 备份组中为 AC 1 配置较高的优先级。

## 3.3 配置注意事项

- 确保 AC 与 RADIUS 服务器的路由可达。
- AC 1 与 AC 2 上，涉及 RADIUS、Domain、Portal、WLAN 等相关配置要保持一致。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

(1) 配置 AC 1 的接口

# 创建 VLAN 10 作为双机热备的 VLAN。

```
<AC1> system-view
[AC1] vlan 10
[AC1-vlan10] quit
```

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 188.10.0.6 16
[AC1-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC1] vlan 200
[AC1-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC1] vlan 300
[AC1-vlan300] quit
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] ip address 188.30.0.6 16
[AC1-Vlan-interface300] quit
```

# 创建 VLAN 400 作为与 RADIUS server 通信的 VLAN，并为该接口配置 IP 地址。

```
[AC1] vlan 400
[AC1-vlan400] quit
[AC1] interface vlan-interface 400
[AC1-Vlan-interface400] ip address 188.40.0.6 16
[AC1-Vlan-interface400] quit
```

# 配置 AC 1 的上行链路 GigabitEthernet1/0/1 接口的链路类型为 Access，并允许 VLAN 400 的报文通过。

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type access
[AC1-GigabitEthernet1/0/1] port access vlan 400
[AC1-GigabitEthernet1/0/1] quit
```

# 配置 AC 1 与 AC 2 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access，当前 Access 口允许 VLAN 10 通过。

```
[AC1] interface gigabitethernet 1/0/2
[AC1-GigabitEthernet1/0/2] port link-type access
[AC1-GigabitEthernet1/0/2] port access vlan 10
[AC1-GigabitEthernet1/0/2] quit
```

# 配置 AC 的下行链路 GigabitEthernet1/0/3 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，并允许 VLAN 100 和 VLAN 300 的报文通过。

```
[AC1] interface gigabitethernet 1/0/3
[AC1-GigabitEthernet1/0/3] port link-type trunk
[AC1-GigabitEthernet1/0/3] port trunk permit vlan 100 300
[AC1-GigabitEthernet1/0/3] port trunk pvid vlan 100
[AC1-GigabitEthernet1/0/3] quit
```

## (2) 配置 MSTP

# 配置生成树的工作模式为 MSTP。

```
[AC1] stp mode mstp
# 激活 MST 域。
[AC1] stp region-configuration
[AC1-mst-region] active region-configuration
[AC1-mst-region] quit
```

# 配置 AC 1 为根桥。

```
[AC1] stp root primary
```

# 使能 STP 功能。

```
[AC1] stp enable
```

## (3) 配置 VRRP

# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 188.30.0.100。

```
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] vrrp vrid 1 virtual-ip 188.30.0.100
```

# 配置 VLAN 接口 300 在 VRRP 备份组 1 中的优先级为 254。

```
[AC1-Vlan-interface300] vrrp vrid 1 priority 254
[AC1-Vlan-interface300] quit
```

# 创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 188.40.0.100。

```
[AC1] interface vlan-interface 400
[AC1-Vlan-interface400] vrrp vrid 2 virtual-ip 188.40.0.100
```

# 配置 VLAN 接口 400 在 VRRP 备份组 2 中的优先级为 254。

```
[AC1-Vlan-interface400] vrrp vrid 2 priority 254
[AC1-Vlan-interface400] quit
```

## (4) 配置 Portal 认证

# 配置 Portal 服务器：名称为 office，IP 地址为 188.30.0.100（VRRP 备份组 1 的虚拟 IP 地址），URL 为 http://188.30.0.100/portal/logon.htm。

```
[AC1] portal server office ip 188.30.0.100 url http://188.30.0.100/portal/logon.htm
```

# 配置本地 Portal 服务器支持 HTTP 协议。

```
[AC1] portal local-server http
```

# 在 VLAN 接口 300 上使能 Portal 认证，并配置为直接认证方式。

```
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] portal server office method direct
[AC1-Vlan-interface300] quit
```

# 创建名为 office 的 RADIUS 方案并进入其视图。

```
[AC1] radius scheme office
```

# 配置 RADIUS 方案的主认证服务器的 IP 地址为 188.40.0.8，认证报文的共享密钥设置为明文 123456。

```
[AC1-radius-office] primary authentication 188.40.0.8
```

```
[AC1-radius-office] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC1-radius-office] user-name-format without-domain
```

```
[AC1-radius-office] quit
```

#### (5) 配置认证域

# 创建名为 office 的 ISP 域，并进入其视图。

```
[AC1] domain office
```

# 配置 Portal 用户使用 RADIUS 方案 office 进行认证，不对用户使用的网络服务进行授权和计费。

```
[AC1-isp-office] authentication portal radius-scheme office
```

```
[AC1-isp-office] authorization portal none
```

```
[AC1-isp-office] accounting portal none
```

# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小数据流量为 1024 个字节。

```
[AC1-isp-office] idle-cut enable 50 1024
```

```
[AC1-isp-office] quit
```

#### (6) 配置 Portal 支持双机热备

# 配置 VLAN 接口 300 属于 Portal 备份组 1。

```
[AC1] interface vlan-interface 300
```

```
[AC1-Vlan-interface300] portal backup-group 1
```

```
[AC1-Vlan-interface300] quit
```

# 配置双机热备模式下的设备 ID 为 1，输入“Y”确认。

```
[AC1] nas device-id 1
```

Warning: This command will cut all user connections on this device. Continue? [Y/N]Y

# 配置发送 RADIUS 报文使用的源 IP 地址为 VRRP 备份组 2 的虚拟 IP 地址。

```
[AC1] radius nas-ip 188.40.0.100
```

# 指定 Portal 用户的认证域为 office。

```
[AC1] interface vlan-interface 300
```

```
[AC1-Vlan-interface300] portal domain office
```

```
[AC1-Vlan-interface300] quit
```

#### (7) 配置 WLAN 服务

# 配置全局备份 AC 的 IP 地址为 188.10.0.7。

```
[AC1] wlan backup-ac ip 188.10.0.7
```

# 使能 AC 间热备份功能。

```
[AC1] hot-backup enable
```

# 配置 AC 间用于热备份的 VLAN 为 VLAN 10。

```
[AC1] hot-backup vlan 10
```

# 创建接口 WLAN-ESS 1，并设置端口的链路类型为 Hybrid。

```
[AC1] interface wlan-ess 1
```

```
[AC1-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。

```
[AC1-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```

[AC1-WLAN-ESS1] mac-vlan enable
[AC1-WLAN-ESS1] quit
# 配置 WLAN 服务模板，SSID 为 service，将接口 WLAN-ESS 1 与该服务模板绑定，并开启 WLAN 服务。
[AC1] wlan service-template 1 clear
[AC1-wlan-st-1] ssid service
[AC1-wlan-st-1] bind wlan-ess 1
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
# 在 AC 1 的 AP 视图下配置 AP 名称为 officeap，型号名称选择 WA2620E-AGN。
[AC1] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC1-wlan-ap-officeap] serial-id 21023529G007C000020
# 配置 AP 的接入优先级设置为 7，该值越大优先级越高，缺省为 4。
[AC1-wlan-ap-officeap] priority level 7
# 进入 radio 2 射频视图。
[AC1-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 300。
[AC1-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC1-wlan-ap-officeap-radio-2] radio enable
[AC1-wlan-ap-officeap-radio-2] quit
[AC1-wlan-ap-officeap] quit
(8) 配置双机热备
# 配置备份 VLAN 为 VLAN 10。
[AC1] dmbk vlan 10
# 使能双机热备功能，且支持对称路径。
[AC1] dmbk enable backup-type symmetric-path

```

### 3.4.2 AC 2 的配置

#### (1) 配置 AC 2 的接口

# 创建 VLAN 10 作为双机热备的 VLAN。

```

<AC2> system-view
[AC2] vlan 10
[AC2-vlan10] quit

```

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```

[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 188.10.0.7 16
[AC2-Vlan-interface100] quit

```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。



```

[AC2] vlan 200
[AC2-vlan200] quit
# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。
[AC2] vlan 300
[AC2-vlan300] quit
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] ip address 188.30.0.7 16
[AC2-Vlan-interface300] quit
# 创建 VLAN 400 作为与 RADIUS server 通信的 VLAN，并为该接口配置 IP 地址。
[AC2] vlan 400
[AC2-vlan400] quit
[AC2] interface vlan-interface 400
[AC2-Vlan-interface400] ip address 188.40.0.7 16
[AC2-Vlan-interface400] quit
# 配置 AC 2 上行链路的 GigabitEthernet1/0/1 接口的链路类型为 Access，并允许 VLAN 400 的报文通过。
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type access
[AC2-GigabitEthernet1/0/1] port access vlan 400
[AC2-GigabitEthernet1/0/1] quit
# 配置 AC 1 与 AC 2 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access，当前 Access 口允许 VLAN 10 通过。
[AC2] interface gigabitethernet 1/0/2
[AC2-GigabitEthernet1/0/2] port link-type access
[AC2-GigabitEthernet1/0/2] port access vlan 10
[AC2-GigabitEthernet1/0/2] quit
# 配置 AC 2 下行链路的 GigabitEthernet1/0/3 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，并允许 VLAN 100 和 VLAN 300 的报文通过。
[AC2] interface gigabitethernet 1/0/3
[AC2-GigabitEthernet1/0/3] port link-type trunk
[AC2-GigabitEthernet1/0/3] port trunk permit vlan 100 300
[AC2-GigabitEthernet1/0/3] port trunk pvid vlan 100
[AC2-GigabitEthernet1/0/3] quit
(2) 配置 MSTP
# 配置生成树的工作模式为 MSTP。
[AC2] stp mode mstp
# 激活 MST 域。
[AC2] stp region-configuration
[AC2-mst-region] active region-configuration
[AC2-mst-region] quit
# 使能 STP 功能。
[AC2] stp enable
(3) 配置 VRRP
# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 188.30.0.100。
[AC2] interface vlan-interface 300

```

```
[AC2-Vlan-interface300] vrrp vrid 1 virtual-ip 188.30.0.100
[AC2-Vlan-interface300] quit
```

# 创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 188.40.0.100。

```
[AC2] interface vlan-interface 400
[AC2-Vlan-interface400] vrrp vrid 2 virtual-ip 188.40.0.100
[AC2-Vlan-interface400] quit
```

#### (4) 配置 Portal 认证

# 配置 Portal 服务器：名称为 office，IP 地址为 188.30.0.100（VRRP 备份组 1 的虚拟 IP 地址），URL 为 http://188.30.0.100/portal/logon.htm。

```
[AC2] portal server office ip 188.30.0.100 url http://188.30.0.100/portal/logon.htm
```

# 配置本地 Portal 服务器支持 HTTP 协议。

```
[AC2] portal local-server http
```

# 在 VLAN 接口 300 上使能 Portal 认证，并配置为直接认证方式。

```
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] portal server office method direct
[AC2-Vlan-interface300] quit
```

# 创建名为 office 的 RADIUS 方案并进入其视图。

```
[AC2] radius scheme office
```

# 配置 RADIUS 方案的主认证服务器的 IP 地址为 188.40.0.8，认证报文的共享密钥设置为明文 123456。

```
[AC2-radius-office] primary authentication 188.40.0.8
[AC2-radius-office] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC2-radius-office] user-name-format without-domain
[AC2-radius-office] quit
```

#### (5) 配置认证域

# 创建名为 office 的 ISP 域，并进入其视图。

```
[AC2] domain office
```

# 配置 Portal 用户使用 RADIUS 方案 office 进行认证，不对用户使用的网络服务进行授权和计费。

```
[AC2-isp-office] authentication portal radius-scheme office
[AC2-isp-office] authorization portal none
[AC2-isp-office] accounting portal none
```

# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小数据流量为 1024 个字节。

```
[AC2-isp-office] idle-cut enable 50 1024
[AC2-isp-office] quit
```

#### (6) 配置 Portal 支持双机热备

# 配置 VLAN 接口 300 属于 Portal 备份组 1。

```
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] portal backup-group 1
[AC2-Vlan-interface300] quit
```

# 配置双机热备模式下的设备 ID 为 2，输入“Y”确认。

```
[AC2] nas device-id 2
```

```
Warning: This command will cut all user connections on this device. Continue? [Y/N]Y
```

# 配置发送 RADIUS 报文使用的源 IP 地址为 VRRP 备份组 2 的虚拟 IP 地址。

```
[AC2] radius nas-ip 188.40.0.100
```

# 指定 portal 用户的认证域为 office。

```
[AC2] interface vlan-interface 300
```

```
[AC2-Vlan-interface300] portal domain office
```

```
[AC2-Vlan-interface300] quit
```

## (7) 配置 WLAN 服务

# 配置全局备份 AC 的 IP 地址为 188.10.0.6。

```
[AC2] wlan backup-ac ip 188.10.0.6
```

# 使能 AC 间热备份功能。

```
[AC2] hot-backup enable
```

# 配置 AC 间用于热备份的 VLAN 为 VLAN 10。

```
[AC2] hot-backup vlan 10
```

# 创建接口 WLAN-ESS 1，并设置端口的链路类型为 Hybrid。

```
[AC2] interface wlan-ess 1
```

```
[AC2-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。

```
[AC2-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
```

```
[AC2-WLAN-ESS1] mac-vlan enable
```

```
[AC2-WLAN-ESS1] quit
```

# 配置 WLAN 服务模板，SSID 为 service，将接口 WLAN-ESS 1 与该服务模板绑定，并开启 WLAN 服务。

```
[AC2] wlan service-template 1 clear
```

```
[AC2-wlan-st-1] ssid service
```

```
[AC2-wlan-st-1] bind wlan-ess 1
```

```
[AC2-wlan-st-1] service-template enable
```

```
[AC2-wlan-st-1] quit
```

# 在 AC 2 的 AP 视图下配置 AP 名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC2] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC2-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC2-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 300。

```
[AC2-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

# 使能 AP 的 radio 2。

```
[AC2-wlan-ap-officeap-radio-2] radio enable
```

```
[AC2-wlan-ap-officeap-radio-2] quit
```

```
[AC2-wlan-ap-officeap] quit
```

## (8) 配置双机热备

# 配置备份 VLAN 为 VLAN 10。

```
[AC2] dhrbk vlan 10
# 使能双机热备功能，且支持对称路径。
[AC2] dhrbk enable backup-type symmetric-path
```

### 3.4.3 Switch 1 的配置

```
# 配置生成树的工作模式为 MSTP。
<Switch1> system-view
[Switch1] stp mode mstp
# 激活 MST 域。
[Switch1] stp region-configuration
[Switch1-mst-region] active region-configuration
[Switch1-mst-region] quit
# 使能 STP 功能。
[Switch1] stp enable
```

### 3.4.4 Switch 2 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线客户端接入的 VLAN。

```
<Switch2> system-view
[Switch2] vlan 100
[Switch2-vlan100] quit
[Switch2] vlan 300
[Switch2-vlan300] quit
```

# 配置 Switch 2 与 AC 1 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch2] interface gigabitethernet 1/0/1
[Switch2-GigabitEthernet1/0/1] port link-type trunk
[Switch2-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch2-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch2-GigabitEthernet1/0/1] quit
```

# 配置 Switch 2 与 AC 2 相连的 GigabitEthernet1/0/2 接口链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch2] interface gigabitethernet 1/0/2
[Switch2-GigabitEthernet1/0/2] port link-type trunk
[Switch2-GigabitEthernet1/0/2] port trunk permit vlan 100 300
[Switch2-GigabitEthernet1/0/2] port trunk pvid vlan 100
[Switch2-GigabitEthernet1/0/2] quit
```

# 配置 Switch 2 与 AP 相连的 GigabitEthernet1/0/3 接口链路类型为 Access，当前 Access 口允许 VLAN 100 通过，并使能 PoE 功能。

```
[Switch2] interface gigabitethernet 1/0/3
[Switch2-GigabitEthernet1/0/3] port link-type access
[Switch2-GigabitEthernet1/0/3] port access vlan 100
[Switch2-GigabitEthernet1/0/3] poe enable
[Switch2-GigabitEthernet1/0/3] quit
```

# 配置生成树的工作模式为 MSTP。

```
[Switch2] stp mode mstp
```

# 激活 MST 域。

```
[Switch2] stp region-configuration
```

```
[Switch2-mst-region] active region-configuration
```

```
[Switch2-mst-region] quit
```

# 使能 STP 功能。

```
[Switch2] stp enable
```

### 3.4.5 RADIUS Server 的配置



说明

下面以 IMC 为例（使用 IMC 版本为：iMC PLAT 7.0 (E0202)、iMC WSM 7.0 (E0202)），说明 Radius Server 的基本配置。

# 增加接入设备

登录进入 IMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入“接入设备配置”页面，在该页面中单击<增加>按钮，进入“增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择接入设备类型为“H3C(General)”；
- 在设备列表中，单击<手工增加>按钮，添加 IP 地址为 188.40.0.100 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 ? 帮助

**接入配置**

|        |              |          |         |
|--------|--------------|----------|---------|
| 认证端口 * | 1812         | 计费端口 *   | 1813    |
| 组网方式   | 不启用混合组网      | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 接入设备分组   | 无       |
| 共享密钥 * | *****        | 确认共享密钥 * | *****   |
| 业务分组   | 未分组          |          |         |

**设备列表**

选择 手工增加 全部清除

| 设备名称 | 设备IP地址       | 设备型号 | 备注 | 删除 |
|------|--------------|------|----|----|
|      | 188.40.0.100 |      |    |    |

共有1条记录。

确定 取消

# 增加接入策略

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入“接入策略管理”页面，单击“增加”按钮，进入“增加接入策略”页面。

- 接入策略名为“portal”，该名称可以自行定义；
- 业务分组选择“未分组”；

- 其他配置采用缺省配置；
- 单击<确定>按钮完成操作。

图3 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略 ? 帮助

基本信息

接入策略名 \*

portal

业务分组 \*

未分组

描述

授权信息

接入时段

无

?

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☒ 不启用
☐ EAP证书认证
☐ WAP证书认证

认证证书类型

EAP-TLS认证

下发VLAN

☐ 下发User Profile

下发用户组

?

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Windows可溶解客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔(分钟)

30

自动重连次数

3

违规处理模式

☒ 下线
☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式

☒ 不限制
☐ 必须静态设置
☐ 必须动态获取

确定

取消

## # 增加接入服务

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入“接入服务管理”页面，点击<增加>按钮，进入“增加接入服务”页面。

- 输入服务名“portal auth”，该名称可以自行定义；
- 业务分组“未分组”；
- 缺省接入策略选择“portal”，即上一步配置的接入策略名；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

基本信息

服务名 \*

portal auth

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

802.1x

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 (PC)

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

# 配置接入用户

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入“接入用户”页面，在该页面中单击<增加>按钮，进入“增加接入用户”页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“admin”；
- 输入证件号码“12345”；
- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图5 增加用户

增加用户

基本信息

用户姓名 \*

admin

证件号码 \*

12345

检查是否可用

通讯地址

电话

电子邮件

用户分组 \*

未分组

确定

取消

在“增加接入用户”页面，按如下方式配置。

- 输入账号名“user”；
- 输入密码“123456”；

- 接入服务选择 “portal auth” ；
- 其他配置保持默认；
- 单击<确定>按钮完成操作。



图6 增加接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

admin

选择

增加用户

帐号名 \*

user

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数里限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                             | 服务后缀 | 状态      | 分配IP地址 |
|-------------------------------------------------|------|---------|--------|
| <input checked="" type="checkbox"/> portal auth |      | 可申<br>请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线SSID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

IP地址

MAC地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

### 3.5 验证配置

# Client 从 AC 1 成功上线后,在 AC 1 上通过命令 **display portal user all** 查看该用户的认证情况。  
可以看到 Portal 用户的工作模式为主用户,表示该用户是由 AC 1 上线。

```
[AC1] display portal user all
Index:1
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:primary
MAC                IP                Vlan    Interface
-----
0021-632f-e4d1     188.30.0.1        300     Vlan-interface300
Total 1 user(s) matched, 1 listed.
```

# Client 从 AC 1 成功上线后,在 AC 2 通过命令 **display portal user all** 查看该用户的认证情况。  
可以看到 Portal 用户的工作模式为备用户,表示该用户的认证信息同步到 AC 2 上。

```
[AC2] display portal user all
Index:0
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:secondary
MAC                IP                Vlan    Interface
-----
0021-632f-e4d1     188.30.0.1        300     Vlan-interface300
Total 1 user(s) matched, 1 listed.
```

# 通过将 AC 1 下电模拟主 AC 宕机的情形,使得 AC 发生主备切换,此时,在 AC 2 上便可以查看到用户的状态由“secondary”转换为“stand-alone”状态,说明此时只有 AC 2 处于工作状态。

```
[AC2] display portal user all
Index:3
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC                IP                Vlan    Interface
-----
0021-632f-e4d1     188.30.0.1        300     Vlan-interface300
Total 1 user(s) matched, 1 listed.
```

### 3.6 配置文件

- AC 1 的配置文件:

```
#
radius nas-ip 188.40.0.100
nas device-id 1
#
portal server office ip 188.30.0.100 url http://188.30.0.100/portal/logon.htm
```

```

portal local-server http
#
wlan backup-ac ip 188.10.0.7
#
hot-backup enable domain 1
hot-backup vlan 10
#
Vlan 10
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
stp instance 0 root primary
stp enable
#
radius scheme office
primary authentication 188.40.0.8
key authentication cipher $c$3$hKKWIPmTANKFS1gsTRFeUQXilk/L11DH/g==
user-name-format without-domain
#
domain office
authentication portal radius-scheme office
authorization portal none
accounting portal none
access-limit disable
state active
idle-cut enable 50 1024
self-service-url disable
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface1
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface100
ip address 188.10.0.6 255.255.0.0
#
interface Vlan-interface300
ip address 188.30.0.6 255.255.0.0
vrrp vrid 1 virtual-ip 188.30.0.100

```

```

vrp vrid 1 priority 254
portal server office method direct
portal domain office
portal backup-group 1
#
interface Vlan-interface400
ip address 188.40.0.6 255.255.0.0
vrp vrid 2 virtual-ip 188.40.0.100
vrp vrid 2 priority 254
#
interface GigabitEthernet1/0/1
port link-type access
port access vlan 400
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 10
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
priority level 7
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1 vlan-id 300
radio enable
#
dhsbk enable backup-type symmetric-path
dhsbk vlan 10
#
• AC 2 的配置文件:
#
nas device-id 2
#
portal server office ip 188.30.0.100 url http://188.30.0.100/portal/logon.htm
portal local-server http
#

```

```

wlan backup-ac ip 188.10.0.6
#
hot-backup enable domain 1
hot-backup vlan 10
#
vlan 10
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
stp enable
#
radius scheme office
primary authentication 188.40.0.8
key authentication cipher $c$3$bN925R2AEzbHlU1DQ/sAebBT9z2cqwdptg==
user-name-format without-domain
#
domain office
authentication portal radius-scheme office
authorization portal none
accounting portal none
access-limit disable
state active
idle-cut enable 50 1024
self-service-url disable
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface1
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface100
ip address 188.10.0.7 255.255.0.0
#
interface Vlan-interface300
ip address 188.30.0.7 255.255.0.0
vrrp vrid 1 virtual-ip 188.30.0.100
portal server office method direct
portal domain office
portal backup-group 1

```

```

#
interface Vlan-interface400
 ip address 188.40.0.7 255.255.0.0
 vrrp vrid 2 virtual-ip 188.40.0.100
#
interface GigabitEthernet1/0/1
 port link-type access
 port access vlan 400
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 10
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 100 300
 port trunk pvid vlan 100
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
 serial-id 21023529G007C000020
 radio 1
 radio 2
 service-template 1 vlan-id 300
 radio enable
#
dhsbk enable backup-type symmetric-path
dhsbk vlan 10
#
• Switch 1 的配置文件:
#
stp enable
#
• Switch 2 的配置文件:
#
vlan 100
#
vlan 300
#
stp enable
#
interface GigabitEthernet1/0/1

```

```
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。

# 双机热备下的 IPv6 本地 Portal 认证典型配置 举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

|                               |    |
|-------------------------------|----|
| 1 简介.....                     | 1  |
| 2 配置前提 .....                  | 1  |
| 3 配置举例 .....                  | 1  |
| 3.1 组网需求 .....                | 1  |
| 3.2 配置思路 .....                | 2  |
| 3.3 配置注意事项.....               | 2  |
| 3.4 配置步骤 .....                | 3  |
| 3.4.1 AC 1 的配置 .....          | 3  |
| 3.4.2 AC 2 的配置 .....          | 7  |
| 3.4.3 Switch 1 的配置 .....      | 12 |
| 3.4.4 Switch 2 的配置 .....      | 12 |
| 3.4.5 RADIUS Server 的配置 ..... | 13 |
| 3.5 验证配置 .....                | 16 |
| 3.6 配置文件 .....                | 17 |
| 4 相关资料 .....                  | 24 |

# 1 简介

本文介绍了双机热备下的本地 Portal 认证典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 无线接入、Portal 认证、双 AC 备份等特性。

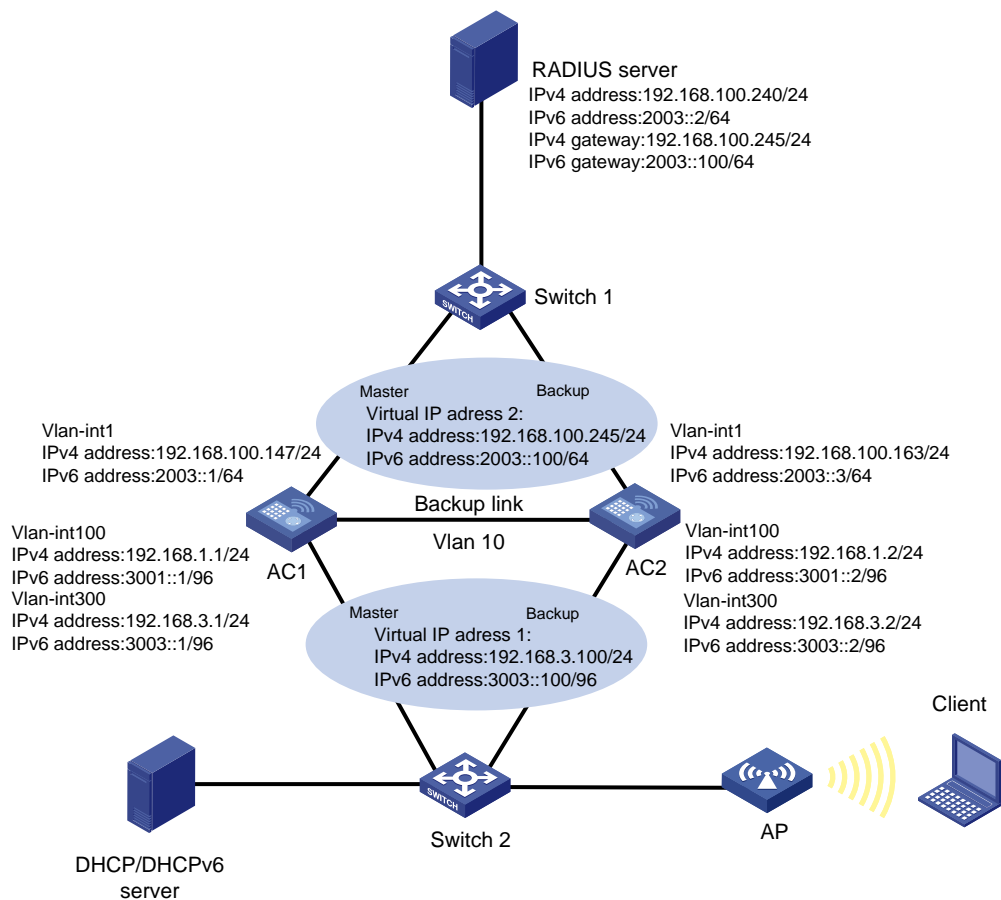
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，为了提高无线用户接入的可靠性，要求在 AC 1 和 AC 2 之间实现双机热备功能，并且对 Portal 用户的数据进行备份。具体需求如下：

- AC1 和 AC2 通过 VLAN 10 传输双机热备报文。
- AC 1 正常工作的情况下，Client 通过 AC 1 进行 Portal 认证接入到外网。AC 1 发生故障的情况下，Client 通过 AC 2 接入到外网，保证业务流量切换不被中断。
- 采用 RADIUS 服务器作为认证/计费服务器，采用 AC 作为本地 Portal 服务器。
- 当 Portal 用户异常下线时，为了防止 AC 误认为异常下线用户仍在线，可以通过用户闲置切断功能来实现。

图1 双机热备下的本地 Portal 认证组网图



## 3.2 配置思路

- 为了避免两台 AC 和上下行设备产生环路，并在主备切换时，尽快完成收敛，需要在 AC 1 和 AC 2 上使能 MSTP 功能，并设置 AC 1 为根桥。
- 当发生主备切换时，为了保证 AC 的上下行不丢包，需要分别在 AC 1 和 AC 2 的上下行接口上配置 VRRP 备份组。
- 为了使 AC 1 成为 VRRP 备份组的 Master AC，需要在 VRRP 备份组中为 AC 1 配置较高的优先级。

## 3.3 配置注意事项

- 确保 AC 与 RADIUS 服务器的路由可达。
- AC 1 与 AC 2 上，涉及 RADIUS、Domain、Portal、WLAN 等的相关配置要保持一致。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

(1) 配置 AC 1 的接口

# 全局使能 IPv6 功能。

```
<AC1> system-view
```

```
[AC1] ipv6
```

# 创建 VLAN 10 作为双机热备的 VLAN。

```
[AC1] vlan 10
```

```
[AC1-vlan10] quit
```

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv4 和 IPv6 地址。AP 将通过该 VLAN 与 AC 建立 LWAPP 隧道。

```
[AC1] vlan 100
```

```
[AC1-vlan100] quit
```

```
[AC1] interface vlan-interface 100
```

```
[AC1-Vlan-interface100] ip address 192.168.1.1 24
```

```
[AC1-Vlan-interface100] ipv6 address 3001::1 96
```

```
[AC1-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC1] vlan 200
```

```
[AC1-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IPv4 和 IPv6 地址。

```
[AC1] vlan 300
```

```
[AC1-vlan300] quit
```

```
[AC1] interface vlan-interface 300
```

```
[AC1-Vlan-interface300] ip address 192.168.3.1 24
```

```
[AC1-Vlan-interface300] ipv6 address fe80::1 link-local
```

```
[AC1-Vlan-interface300] ipv6 address 3003::1 96
```

```
[AC1-Vlan-interface300] quit
```

# 创建 VLAN 1 作为与 RADIUS server 通信的 VLAN，并为该接口配置 IPv4 和 IPv6 地址。

```
[AC1] vlan 1
```

```
[AC1-vlan1] quit
```

```
[AC1] interface vlan-interface 1
```

```
[AC1-Vlan-interface1] ip address 192.168.100.147 24
```

```
[AC1-Vlan-interface1] ipv6 address fe80::2 link-local
```

```
[AC1-Vlan-interface1] ipv6 address 2003::1 64
```

```
[AC1-Vlan-interface1] quit
```

# 配置 AC 1 与 AC 2 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access，当前 Access 口允许 VLAN 10 通过。

```
[AC1] interface gigabitethernet 1/0/2
```

```
[AC1-GigabitEthernet1/0/2] port link-type access
```

```
[AC1-GigabitEthernet1/0/2] port access vlan 10
```

```
[AC1-GigabitEthernet1/0/2] quit
```

# 配置 AC1 的下行链路 GigabitEthernet1/0/3 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，并允许 VLAN 100 和 VLAN 300 的报文通过。

```
[AC1] interface gigabitethernet 1/0/3
[AC1-GigabitEthernet1/0/3] port link-type trunk
[AC1-GigabitEthernet1/0/3] port trunk permit vlan 100 300
[AC1-GigabitEthernet1/0/3] port trunk pvid vlan 100
[AC1-GigabitEthernet1/0/3] quit
```

## (2) 配置 MSTP

# 配置生成树的工作模式为 MSTP。

```
[AC1] stp mode mstp
# 激活 MST 域。
[AC1] stp region-configuration
[AC1-mst-region] active region-configuration
[AC1-mst-region] quit
```

# 配置 AC 1 为根桥。

```
[AC1] stp root primary
```

# 使能 STP 功能。

```
[AC1] stp enable
```

## (3) 配置 VRRP

# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IPv4 地址为 192.168.3.100，虚拟 IPv6 地址为 FE80::30 和 3003::100。

```
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] vrrp vrid 1 virtual-ip 192.168.3.100
[AC1-Vlan-interface300] vrrp ipv6 vrid 1 virtual-ip fe80::30 link-local
[AC1-Vlan-interface300] vrrp ipv6 vrid 1 virtual-ip 3003::100
```

# 配置 VLAN 接口 300 在 VRRP 备份组 1 中的优先级为 254。

```
[AC1-Vlan-interface300] vrrp vrid 1 priority 254
[AC1-Vlan-interface300] vrrp ipv6 vrid 1 priority 254
[AC1-Vlan-interface300] quit
```

# 创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IPv4 地址为 192.168.100.245，虚拟 IPv6 地址为 FE80::40 和 2003::100。

```
[AC1] interface vlan-interface 1
[AC1-Vlan-interface1] vrrp vrid 2 virtual-ip 192.168.100.245
[AC1-Vlan-interface1] vrrp ipv6 vrid 2 virtual-ip fe80::40 link-local
[AC1-Vlan-interface1] vrrp ipv6 vrid 2 virtual-ip 2003::100
```

# 配置 VLAN 接口 1 在 VRRP 备份组 2 中的优先级为 254。

```
[AC1-Vlan-interface1] vrrp vrid 2 priority 254
[AC1-Vlan-interface1] vrrp ipv6 vrid 2 priority 254
[AC1-Vlan-interface400] quit
```

## (4) 配置 Portal 认证

# 配置 IPv4 Portal 服务器：名称为 officev4，IPv4 地址为 192.168.3.100（VRRP 备份组 1 的虚拟 IPv4 地址），URL 为 http://192.168.3.100/portal/logon.htm。

```
[AC1] portal server officev4 ip 192.168.3.100 url http://192.168.3.100/portal/logon.htm
```

# 配置 IPv6 Portal 服务器：名称为 officev6，IPv6 地址为 3003::100（VRRP 备份组 1 的虚拟 IPv6 地址），URL 为 http://[3003::100]/portal/logon.htm。

```
[AC1] portal server officev6 ipv6 3003::100 url http://[3003::100]/portal/logon.htm
```

# 配置本地 Portal 服务器支持 HTTP 协议。

```
[AC1] portal local-server http
```

# 在 VLAN 接口 300 上配置 Portal 用户报文的控制模式为 MAC，IPv4 或者 IPv6 用户通过 Portal 认证上线后，同时允许该用户的 IPv4 和 IPv6 报文通过认证接口。

```
[AC1] interface vlan-interface 300
```

```
[AC1-Vlan-interface300] portal control-mode mac
```

# 在 VLAN 接口 300 上使能 Portal 认证，并配置为直接认证方式。

```
[AC1-Vlan-interface300] portal server officev4 method direct
```

```
[AC1-Vlan-interface300] portal server officev6 method direct
```

```
[AC1-Vlan-interface300] quit
```

#### (5) 配置 IPv4 RADIUS 方案

# 创建名为 rs4 的 RADIUS 方案并进入其视图。

```
[AC1] radius scheme rs4
```

# 配置 RADIUS 方案的主认证服务器的 IPv4 地址为 192.168.100.240，认证报文的共享密钥设置为明文 123456。

```
[AC1-radius-rs4] primary authentication 192.168.100.240
```

```
[AC1-radius-rs4] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC1-radius-rs4] user-name-format without-domain
```

```
[AC1-radius-rs4] quit
```

#### (6) 配置 IPv6 RADIUS 方案

# 创建名为 rs6 的 RADIUS 方案并进入其视图。

```
[AC1] radius scheme rs6
```

# 配置 RADIUS 方案的主认证服务器的 IPv6 地址为 2003::2，认证报文的共享密钥设置为明文 123456。

```
[AC1-radius-rs6] primary authentication ipv6 2003::2
```

```
[AC1-radius-rs6] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC1-radius-rs6] user-name-format without-domain
```

```
[AC1-radius-rs6] quit
```

#### (7) 配置 IPv4 认证域

# 创建名为 dm4 的 ISP 域，并进入其视图。

```
[AC1] domain dm4
```

# 配置 Portal 用户使用 RADIUS 方案 rs4 进行认证，不对用户使用的网络服务进行授权和计费。

```
[AC1-isp-dm4] authentication portal radius-scheme rs4
```

```
[AC1-isp-dm4] authorization portal none
```

```
[AC1-isp-dm4] accounting portal none
```

# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小数据流量为 1024 个字节。

```
[AC1-isp-dm4] idle-cut enable 50 1024
```

```
[AC1-isp-dm4] quit
```

#### (8) 配置 IPv6 认证域

# 创建名为 dm6 的 ISP 域，并进入其视图。

```
[AC1] domain dm6
```

# 配置 Portal 用户使用 RADIUS 方案 rs6 进行认证，不对用户使用的网络服务进行授权和计费。

```

[AC1-isp-dm6] authentication portal radius-scheme rs6
[AC1-isp-dm6] authorization portal none
[AC1-isp-dm6] accounting portal none
# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小
数据流量为 1024 个字节。
[AC1-isp-dm6] idle-cut enable 50 1024
[AC1-isp-dm6] quit
(9) 配置 Portal 支持双机热备
# 配置 VLAN 接口 300 属于 Portal 备份组 1。
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] portal backup-group 1
[AC1-Vlan-interface300] quit
# 配置双机热备模式下的设备 ID 为 1，输入“Y”确认。
[AC1] nas device-id 1
Warning: This command will cut all user connections on this device. Continue? [Y/N]Y
# 配置发送 RADIUS 报文使用的源 IPv4 地址为 VRRP 备份组 2 的虚拟 IPv4 地址。
[AC1] radius nas-ip 192.168.100.245
# 配置发送 RADIUS 报文使用的源 IPv6 地址为 VRRP 备份组 2 的虚拟 IPv6 地址。
[AC1] radius nas-ip ipv6 2003::100
# 指定 IPv4 Portal 用户的认证域为 dm4。
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] portal domain dm4
# 指定 IPv6 Portal 用户的认证域为 dm6。
[AC1-Vlan-interface300] portal domain ipv6 dm6
[AC1-Vlan-interface300] quit
(10) 配置 WLAN 服务
# 配置全局备份 AC 的 IPv4 地址为 192.168.1.2。
[AC1] wlan backup-ac ip 192.168.1.2
# 配置全局备份 AC 的 IPv6 地址为 3001::2。
[AC1] wlan backup-ac ipv6 3001::2
# 使能 AC 间热备份功能。
[AC1] hot-backup enable
# 配置 AC 间用于热备份的 VLAN 为 VLAN 10。
[AC1] hot-backup vlan 10
# 创建接口 WLAN-ESS 1，并设置端口的链路类型为 Hybrid。
[AC1] interface wlan-ess 1
[AC1-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 和 VLAN 300
不带 Tag 通过。
[AC1-WLAN-ESS1] undo port hybrid vlan 1
[AC1-WLAN-ESS1] port hybrid vlan 200 300 untagged
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
# 使能 MAC VLAN 功能。
[AC1-WLAN-ESS1] mac-vlan enable

```

```

[AC1-WLAN-ESS1] quit
# 配置 WLAN 服务模板，SSID 为 service，将接口 WLAN-ESS 1 与该服务模板绑定，并开启 WLAN 服务。
[AC1] wlan service-template 1 clear
[AC1-wlan-st-1] ssid service
[AC1-wlan-st-1] bind wlan-ess 1
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
# 在 AC 1 的 AP 视图下配置 AP 名称为 officeap，型号名称选择 WA2620E-AGN。
[AC1] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC1-wlan-ap-officeap] serial-id 21023529G007C000020
# 配置 AP 的接入优先级设置为 7，该值越大优先级越高，缺省为 4。
[AC1-wlan-ap-officeap] priority level 7
# 进入 radio 2 射频视图。
[AC1-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 300。
[AC1-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC1-wlan-ap-officeap-radio-2] radio enable
[AC1-wlan-ap-officeap-radio-2] quit
[AC1-wlan-ap-officeap] quit
(11) 配置双机热备
# 配置备份 VLAN 为 VLAN 10。
[AC1] dmbk vlan 10
# 使能双机热备功能，且支持对称路径。
[AC1] dmbk enable backup-type symmetric-path

```

### 3.4.2 AC 2 的配置

#### (1) 配置 AC 2 的接口

```

# 全局使能 IPv6 功能。
<AC2> system-view
[AC2] ipv6
# 创建 VLAN 10 作为双机热备的 VLAN。
[AC2] vlan 10
[AC2-vlan10] quit
# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv4 和 IPv6 地址。AP 将通过该 VLAN 与 AC 建立 LWAPP 隧道。
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 192.168.1.2 24
[AC2-Vlan-interface100] ipv6 address 3001::2 96

```



```

[AC2-Vlan-interface100] quit
# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。
[AC2] vlan 200
[AC2-vlan200] quit
# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IPv4 和 IPv6 地址。
[AC2] vlan 300
[AC2-vlan300] quit
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] ip address 192.168.3.2 24
[AC2-Vlan-interface300] ipv6 address fe80::3 link-local
[AC2-Vlan-interface300] ipv6 address 3003::2 96
[AC2-Vlan-interface300] quit
# 创建 VLAN 1 作为与 RADIUS server 通信的 VLAN，并为该接口配置 IPv4 和 IPv6 地址。
[AC2] vlan 1
[AC2-vlan1] quit
[AC2] interface vlan-interface 1
[AC2-Vlan-interface1] ip address 192.168.100.163 24
[AC2-Vlan-interface1] ipv6 address fe80::4 link-local
[AC2-Vlan-interface1] ipv6 address 2003::3 64
[AC2-Vlan-interface1] quit
# 配置 AC 1 与 AC 2 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access，当前 Access 口允许 VLAN 10 通过。
[AC2] interface gigabitethernet 1/0/2
[AC2-GigabitEthernet1/0/2] port link-type access
[AC2-GigabitEthernet1/0/2] port access vlan 10
[AC2-GigabitEthernet1/0/2] quit
# 配置 AC 2 下行链路的 GigabitEthernet1/0/3 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，并允许 VLAN 100 和 VLAN 300 的报文通过。
[AC2] interface gigabitethernet 1/0/3
[AC2-GigabitEthernet1/0/3] port link-type trunk
[AC2-GigabitEthernet1/0/3] port trunk permit vlan 100 300
[AC2-GigabitEthernet1/0/3] port trunk pvid vlan 100
[AC2-GigabitEthernet1/0/3] quit
(2) 配置 MSTP
# 配置生成树的工作模式为 MSTP。
[AC2] stp mode mstp
# 激活 MST 域。
[AC2] stp region-configuration
[AC2-mst-region] active region-configuration
[AC2-mst-region] quit
# 使能 STP 功能。
[AC2] stp enable
(3) 配置 VRRP
# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IPv4 地址为 192.168.3.100，虚拟 IPv6 地址为 FE80::30 和 3003::100。

```

```
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] vrrp vrid 1 virtual-ip 192.168.3.100
[AC2-Vlan-interface300] vrrp ipv6 vrid 1 virtual-ip fe80::30 link-local
[AC2-Vlan-interface300] vrrp ipv6 vrid 1 virtual-ip 3003::100
[AC2-Vlan-interface300] quit
```

# 创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IPv4 地址为 192.168.100.245，虚拟 IPv6 地址为 FE80::40 和 2003::100。

```
[AC2] interface vlan-interface 1
[AC2-Vlan-interface1] vrrp vrid 2 virtual-ip 192.168.100.245
[AC2-Vlan-interface1] vrrp ipv6 vrid 2 virtual-ip fe80::40 link-local
[AC2-Vlan-interface1] vrrp ipv6 vrid 2 virtual-ip 2003::100
[AC2-Vlan-interface1] quit
```

#### (4) 配置 Portal 认证

# 配置 IPv4 Portal 服务器：名称为 officev4，IPv4 地址为 192.168.3.100（VRRP 备份组 1 的虚拟 IPv4 地址），URL 为 http://192.168.3.100/portal/logon.htm。

```
[AC2] portal server officev4 ip 192.168.3.100 url http://192.168.3.100/portal/logon.htm
```

# 配置 IPv6 Portal 服务器：名称为 officev6，IPv6 地址为 3003::100（VRRP 备份组 1 的虚拟 IPv6 地址），URL 为 http://[3003::100]/portal/logon.htm。

```
[AC1] portal server officev6 ipv6 3003::100 url http://[3003::100]/portal/logon.htm
```

# 配置本地 Portal 服务器支持 HTTP 协议。

```
[AC2] portal local-server http
```

# 在 VLAN 接口 300 上配置 Portal 用户报文的控制模式为 MAC，IPv4 或者 IPv6 用户通过 Portal 认证上线后，同时允许该用户的 IPv4 和 IPv6 报文通过认证接口。

```
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] portal control-mode mac
```

# 在 VLAN 接口 300 上使能 Portal 认证，并配置为直接认证方式。

```
[AC2-Vlan-interface300] portal server officev4 method direct
[AC2-Vlan-interface300] portal server officev6 method direct
[AC2-Vlan-interface300] quit
```

#### (5) 配置 IPv4 RADIUS 方案

# 创建名为 rs4 的 RADIUS 方案并进入其视图。

```
[AC2] radius scheme rs4
```

# 配置 RADIUS 方案的主认证服务器的 IPv4 地址为 192.168.100.240，认证报文的共享密钥设置为明文 123456。

```
[AC2-radius-rs4] primary authentication 192.168.100.240
[AC2-radius-rs4] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC2-radius-rs4] user-name-format without-domain
[AC2-radius-rs4] quit
```

#### (6) 配置 IPv6 RADIUS 方案

# 创建名为 rs6 的 RADIUS 方案并进入其视图。

```
[AC2] radius scheme rs6
```

# 配置 RADIUS 方案的主认证服务器的 IPv6 地址为 2003::2，认证报文的共享密钥设置为明文 123456。

```
[AC2-radius-rs6] primary authentication ipv6 2003::2
[AC2-radius-rs6] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC2-radius-rs6] user-name-format without-domain
[AC2-radius-rs6] quit
```

#### (7) 配置 IPv4 认证域

# 创建名为 dm4 的 ISP 域，并进入其视图。

```
[AC2] domain dm4
```

# 配置 Portal 用户使用 RADIUS 方案 rs4 进行认证，不对用户使用的网络服务进行授权和计费。

```
[AC2-isp-dm4] authentication portal radius-scheme rs4
[AC2-isp-dm4] authorization portal none
[AC2-isp-dm4] accounting portal none
```

# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小数据流量为 1024 个字节。

```
[AC2-isp-dm4] idle-cut enable 50 1024
[AC2-isp-dm4] quit
```

#### (8) 配置 IPv6 认证域

# 创建名为 dm6 的 ISP 域，并进入其视图。

```
[AC2] domain dm6
```

# 配置 Portal 用户使用 RADIUS 方案 rs6 进行认证，不对用户使用的网络服务进行授权和计费。

```
[AC2-isp-dm6] authentication portal radius-scheme rs6
[AC2-isp-dm6] authorization portal none
[AC2-isp-dm6] accounting portal none
```

# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小数据流量为 1024 个字节。

```
[AC2-isp-dm6] idle-cut enable 50 1024
[AC2-isp-dm6] quit
```

#### (9) 配置 Portal 支持双机热备

# 配置 VLAN 接口 300 属于 Portal 备份组 1。

```
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] portal backup-group 1
[AC2-Vlan-interface300] quit
```

# 配置双机热备模式下的设备 ID 为 2，输入“Y”确认。

```
[AC2] nas device-id 2
```

Warning: This command will cut all user connections on this device. Continue? [Y/N]Y

# 配置发送 RADIUS 报文使用的源 IPv4 地址为 VRRP 备份组 2 的虚拟 IPv4 地址。

```
[AC2] radius nas-ip 192.168.100.245
```

# 配置发送 RADIUS 报文使用的源 IPv6 地址为 VRRP 备份组 2 的虚拟 IPv6 地址。

```
[AC1] radius nas-ip ipv6 2003::100
```

# 指定 IPv4 portal 用户的认证域为 dm4。

```
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] portal domain dm4
```

# 指定 IPv6 Portal 用户的认证域为 dm6。

```
[AC2-Vlan-interface300] portal domain ipv6 dm6
```

```
[AC2-Vlan-interface300] quit
```

## (10) 配置 WLAN 服务

# 配置全局备份 AC 的 IPv4 地址为 192.168.1.1。

```
[AC2] wlan backup-ac ip 192.168.1.1
```

# 配置全局备份 AC 的 IPv6 地址为 3001::1。

```
[AC1] wlan backup-ac ipv6 3001::1
```

# 使能 AC 间热备份功能。

```
[AC2] hot-backup enable
```

# 配置 AC 间用于热备份的 VLAN 为 VLAN 10。

```
[AC2] hot-backup vlan 10
```

# 创建接口 WLAN-ESS 1，并设置端口的链路类型为 Hybrid。

```
[AC2] interface wlan-ess 1
```

```
[AC2-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。

```
[AC2-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC2-WLAN-ESS1] port hybrid vlan 200 300 untagged
```

```
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
```

```
[AC2-WLAN-ESS1] mac-vlan enable
```

```
[AC2-WLAN-ESS1] quit
```

# 配置 WLAN 服务模板，SSID 为 service，将接口 WLAN-ESS 1 与该服务模板绑定，并开启 WLAN 服务。

```
[AC2] wlan service-template 1 clear
```

```
[AC2-wlan-st-1] ssid service
```

```
[AC2-wlan-st-1] bind wlan-ess 1
```

```
[AC2-wlan-st-1] service-template enable
```

```
[AC2-wlan-st-1] quit
```

# 在 AC 2 的 AP 视图下配置 AP 名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC2] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC2-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC2-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 300。

```
[AC2-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

# 使能 AP 的 radio 2。

```
[AC2-wlan-ap-officeap-radio-2] radio enable
```

```
[AC2-wlan-ap-officeap-radio-2] quit
```

```
[AC2-wlan-ap-officeap] quit
```

## (11) 配置双机热备

# 配置备份 VLAN 为 VLAN 10。

```
[AC2] dhrbk vlan 10
```

# 使能双机热备功能，且支持对称路径。

```
[AC2] dhrbk enable backup-type symmetric-path
```

### 3.4.3 Switch 1 的配置

```
# 全局使能 IPv6 功能。
<Switch1> system-view
[Switch1] ipv6
# 配置生成树的工作模式为 MSTP。
[Switch1] stp mode mstp
# 激活 MST 域。
[Switch1] stp region-configuration
[Switch1-mst-region] active region-configuration
[Switch1-mst-region] quit
# 使能 STP 功能。
[Switch1] stp enable
```

### 3.4.4 Switch 2 的配置

#### (1) 配置 Switch2 的接口

```
# 全局使能 IPv6 功能。
<Switch2> system-view
[Switch2] ipv6
# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。
[Switch2] vlan 100
[Switch2-vlan100] quit
[Switch2] vlan 300
[Switch2-vlan300] quit
# 配置 Switch 2 与 AC 1 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。
[Switch2] interface gigabitethernet 1/0/1
[Switch2-GigabitEthernet1/0/1] port link-type trunk
[Switch2-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch2-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch2-GigabitEthernet1/0/1] quit
# 配置 Switch 2 与 AC 2 相连的 GigabitEthernet1/0/2 接口链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。
[Switch2] interface gigabitethernet 1/0/2
[Switch2-GigabitEthernet1/0/2] port link-type trunk
[Switch2-GigabitEthernet1/0/2] port trunk permit vlan 100 300
[Switch2-GigabitEthernet1/0/2] port trunk pvid vlan 100
[Switch2-GigabitEthernet1/0/2] quit
# 配置 Switch 2 与 AP 相连的 GigabitEthernet1/0/3 接口链路类型为 Access, 当前 Access 口允许 VLAN 100 通过, 并使能 PoE 功能。
[Switch2] interface gigabitethernet 1/0/3
[Switch2-GigabitEthernet1/0/3] port link-type access
[Switch2-GigabitEthernet1/0/3] port access vlan 100
[Switch2-GigabitEthernet1/0/3] poe enable
```

```
[Switch2-GigabitEthernet1/0/3] quit
# 配置生成树的工作模式为 MSTP。
[Switch2] stp mode mstp
# 激活 MST 域。
[Switch2] stp region-configuration
[Switch2-mst-region] active region-configuration
[Switch2-mst-region] quit
# 使能 STP 功能。
[Switch2] stp enable
```

### 3.4.5 RADIUS Server 的配置



说明

下面以 IMC 为例（使用 IMC 版本为：iMC PLAT 7.1(E0303)、iMC EIA 7.1(E0304)、iMC EIP 7.1(E0304)），说明 Radius Server 的基本配置。

#### # 增加接入设备

登录进入 IMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入“接入设备配置”页面，在该页面中单击<增加>按钮，进入“增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择接入设备类型为“H3C(General)”；
- 在设备列表中，单击<手工增加>按钮，添加 IP 地址为 192.168.100.245 的接入设备；
- 单击<增加 IPv6 设备>按钮，进入“手工增加接入设备”页面，填写起始 IP 地址为 2003::100，单击<确定>按钮完成操作；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加 IPv4 接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \*

1812

业务类型

LAN接入业务

接入设备类型

H3C(General)

共享密钥 \*

.....

接入设备分组

无

证书认证

☒不启用 ☐EAP证书认证 ☐WAP证书认证

认证证书类型

EAP-TLS认证

计费端口 \*

1813

业务分组

未分组

确认共享密钥 \*

.....

设备列表

选择手工增加增加IPv6设备全部清除

| 设备名称 | 设备IP地址          | 设备型号 | 备注 | 删除 |
|------|-----------------|------|----|----|
|      | 192.168.100.245 |      |    |    |

图3 增加 IPv6 接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \*

1812

业务类型

LAN接入业务

接入设备类型

H3C(General)

共享密钥 \*

.....

接入设备分组

无

证书认证

☒不启用 ☐EAP证书认证 ☐WAP证书认证

认证证书类型

EAP-TLS认证

计费端口 \*

1813

业务分组

未分组

确认共享密钥 \*

.....

设备列表

选择手工增加增加IPv6设备全部清除

| 设备名称 | 设备IP地址                                  | 设备型号 | 备注 | 删除 |
|------|-----------------------------------------|------|----|----|
|      | 2003:0000:0000:0000:0000:0000:0000:0100 |      |    |    |

# 增加接入策略

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入“接入策略管理”页面，单击“增加”按钮，进入“增加接入策略”页面。

- 接入策略名为“portal”，该名称可以自行定义；
- 业务分组选择“未分组”；
- 其他配置采用缺省配置；
- 单击<确定>按钮完成操作。

图4 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略 帮助

基本信息

接入策略名 \*

portal

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

下发VLAN

☐ 下发User Profile

下发用户组

☐ 下发ACL

# 增加接入服务

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入“接入服务管理”页面，点击<增加>按钮，进入“增加接入服务”页面。

- 输入服务名“portal auth”，该名称可以自行定义；
- 业务分组“未分组”；
- 缺省接入策略选择“portal”，即上一步配置的接入策略名；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

基本信息

服务名 \*

portal auth

业务分组 \*

未分组

缺省私有属性下发策略 \*

不使用

缺省单帐号最大绑定终端数 \*

0

服务描述

☒ 可申请

服务后缀

缺省接入策略 \*

portal

缺省单帐号在线数量限制 \*

0

☒ 无感知认证

# 配置接入用户

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入“接入用户”页面，在该页面中单击<增加>按钮，进入“增加接入用户”页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“admin”；
- 输入证件号码“12345”；
- 单击<检查是否可用>按钮；



- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图6 增加用户

增加用户

基本信息

用户姓名 \*

admin

✓

证件号码 \*

12345

✓

检查是否可用

通讯地址

电话

?

电子邮件

?

用户分组 \*

未分组

确定

取消

在“增加接入用户”页面，按如下方式配置。

- 输入账号名“portal”；
- 输入密码“123456”；
- 接入服务选择“portal auth”；
- 其他配置保持默认；
- 单击<确定>按钮完成操作。

图7 增加接入用户

接入信息

用户姓名 \*

admin

选择

增加用户

帐号名 \*

portal

☐ 预开户用户

☐ 缺省BYOD用户

☐ MAC地址认证用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

时

失效时间

时

最大闲置时长(分钟)

在线数量限制

1

登录提示信息

接入服务

| 服务名                                             | 服务后缀 | 状态  | 分配IP地址 |
|-------------------------------------------------|------|-----|--------|
| <input type="checkbox"/> dot1x-w                |      | 可申请 |        |
| <input checked="" type="checkbox"/> portal auth |      | 可申请 |        |

### 3.5 验证配置

# Client 从 AC 1 成功上线后，在 AC 1 上通过命令 **display portal user all** 查看该用户的认证情况。可以看到 Portal 用户的工作模式为主用户，表示该用户是由 AC 1 上线。

```
[AC1] display portal user all
Index:1
```

```

State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:primary
MAC              IP              Vlan    Interface
-----
0021-632f-e4d1   192.168.3.5      300     Vlan-interface300
Total 1 user(s) matched, 1 listed.

```

# Client 从 AC 1 成功上线后，在 AC 2 通过命令 **display portal user all** 查看该用户的认证情况。可以看到 Portal 用户的工作模式为备用户，表示该用户的认证信息同步到 AC 2 上。

```

[AC2] display portal user all
Index:0
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:secondary
MAC              IP              Vlan    Interface
-----
0021-632f-e4d1   192.168.3.5      300     Vlan-interface300
Total 1 user(s) matched, 1 listed.

```

# 通过将 AC 1 下电模拟主 AC 宕机的情形，使得 AC 发生主备切换，此时，在 AC 2 上便可以查看到用户的状态由“secondary”转换为“stand-alone”状态，说明此时只有 AC 2 处于工作状态。

```

[AC2] display portal user all
Index:3
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC              IP              Vlan    Interface
-----
0021-632f-e4d1   192.168.3.5      300     Vlan-interface300
Total 1 user(s) matched, 1 listed.

```

## 3.6 配置文件

- AC 1 的配置文件：

```

#
radius nas-ip ipv6 2003::0100
nas device-id 1
#
ipv6
#
portal server officev6 ipv6 3003::100 url http://[3003::100]/portal/logon.htm s
erver-type imc
portal server officev4 ip 192.168.3.100 url http://192.168.3.100/portal/logon.h
tm server-type imc
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any

```

```

portal local-server http
#
wlan backup-ac ip 192.168.1.2
wlan backup-ac ipv6 3001::2
#
hot-backup enable domain 1
hot-backup vlan 10
#
vlan 1
#
vlan 10
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme rs6
primary authentication ipv6 2003::0002
primary accounting ipv6 2003::0002
key authentication cipher $c$3$YvYFuVf9PIY6Jg/eYeuH7VLV0vbhAmh0gg==
user-name-format without-domain
radius scheme rs4
primary authentication 192.168.100.240
primary accounting 192.168.100.240
key authentication cipher $c$3$zdQLHG1FGgNpAuye0JS3331P6s0KQNvmrw==
key accounting cipher $c$3$OIc+iiVqnz13BQBHa/LiDTlVVIFQ0RbZJA==
user-name-format without-domain
#
domain dm4
authentication portal radius-scheme rs4
authorization portal none
accounting portal none
access-limit disable
state active
idle-cut enable 50 1024
self-service-url disable
domain dm6
authentication portal radius-scheme rs6
authorization portal none
accounting portal none
access-limit disable
state active
idle-cut enable 50 1024
self-service-url disable
#
stp instance 0 root primary

```

```

stp enable
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface1
ipv6 address 2003::1/64
ipv6 address FE80::2 link-local
ip address 192.168.100.147 255.255.255.0
vrrp vrid 2 virtual-ip 192.168.100.245
vrrp vrid 2 priority 254
vrrp ipv6 vrid 2 virtual-ip FE80::40 link-local
vrrp ipv6 vrid 2 virtual-ip 2003::100
vrrp ipv6 vrid 2 priority 254
#
interface Vlan-interface10
ipv6 address 3010::1/96
ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface100
ipv6 address 3001::1/96
ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface200
#
interface Vlan-interface300
ipv6 address 3003::1/96
ipv6 address FE80::1 link-local
ip address 192.168.3.1 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.3.100
vrrp vrid 1 priority 254
vrrp ipv6 vrid 1 virtual-ip FE80::30 link-local
vrrp ipv6 vrid 1 virtual-ip 3003::100
vrrp ipv6 vrid 1 priority 254
portal control-mode mac
portal server officev4 method direct
portal server officev6 method direct
portal domain dm4
portal domain ipv6 dm6
portal backup-group 1
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 300
#
interface GigabitEthernet1/0/2

```

```

port link-type trunk
port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/3
port access vlan 10
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 300 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio enable
radio 2
service-template 1 vlan-id 300
radio enable
#
dhsbk enable backup-type symmetric-path
dhsbk vlan 10
#
return

```

- AC 2 的配置文件:

```

#
radius nas-ip ipv6 2003::0100
nas device-id 2
#
ipv6
#
portal server officev4 ip 192.168.3.100 url http://192.168.3.100/portal/logon.htm
server-type imc
portal server officev6 ipv6 3003::100 url http://[3003::100]/portal/logon.htm
server-type imc
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
portal local-server http
#
wlan backup-ac ip 192.168.1.1
wlan backup-ac ipv6 3001::1
#
hot-backup enable domain 1
hot-backup vlan 10
#
vlan 1
#
vlan 10

```

```

#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme rs4
  primary authentication 192.168.100.240
  key authentication cipher $c$3$ezwUorHFXLxU0eaO2OyoyURVFuZwUNflAA==
  user-name-format without-domain
radius scheme rs6
  primary authentication ipv6 2003::0002
  key authentication cipher $c$3$+qsA4GoP0aSDprsQyjFcsijBFDr2wsISTg==
  user-name-format without-domain
#
domain dm4
  authentication portal radius-scheme rs4
  authorization portal none
  accounting portal none
  access-limit disable
  state active
  idle-cut enable 50 1024
  self-service-url disable
domain dm6
  authentication portal radius-scheme rs6
  authorization portal none
  accounting portal none
  access-limit disable
  state active
  idle-cut enable 50 1024
  self-service-url disable
#
  stp enable
#
wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable
#
interface NULL0
#
interface Vlan-interface1
  ipv6 address 2003::3/64
  ipv6 address FE80::4 link-local
  ip address 192.168.100.163 255.255.255.0
  vrrp vrid 2 virtual-ip 192.168.100.245
  vrrp ipv6 vrid 2 virtual-ip FE80::40 link-local

```

```

vrp ipv6 vrid 2 virtual-ip 2003::100
#
interface Vlan-interface10
  ipv6 address 3010::2/96
  ip address 192.168.10.2 255.255.255.0
#
interface Vlan-interface100
  ipv6 address 3001::2/96
  ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface200
#
interface Vlan-interface300
  ipv6 address 3003::2/96
  ipv6 address FE80::3 link-local
  ip address 192.168.3.2 255.255.255.0
  vrrp vrid 1 virtual-ip 192.168.3.100
  vrrp ipv6 vrid 1 virtual-ip FE80::30 link-local
  vrrp ipv6 vrid 1 virtual-ip 3003::100
  portal control-mode mac
  portal server officev4 method direct
  portal server officev6 method direct
  portal domain dm4
  portal domain ipv6 dm6
  portal backup-group 1
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 300
#
interface GigabitEthernet1/0/2
  port link-type trunk
  port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/3
  port access vlan 10
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 300 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2

```

```

service-template 1 vlan-id 300
radio enable
#
dhbk enable backup-type symmetric-path
dhbk vlan 10
#
return

```

- Switch 1 的配置文件:

```

#
stp enable
#

```

- Switch 2 的配置文件:

```

dhcp enable
#
ipv6 dhcp server forbidden-address 3001::1 3001::4
ipv6 dhcp server forbidden-address 3003::1 3003::4
#
#
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#
stp global enable
#
dhcp server ip-pool 100
network 192.168.1.0 mask 255.255.255.0
#
dhcp server ip-pool 300
network 192.168.3.0 mask 255.255.255.0
#
ipv6 dhcp pool 1
network 3001::/96
#
ipv6 dhcp pool 2
network 3003::/96
#
ipv6 dhcp pool global
#
interface NULL0
#
interface Vlan-interface100
ip address 192.168.1.3 255.255.255.0
ipv6 dhcp select server
ipv6 dhcp server apply pool 1

```



```

ipv6 address 3001::3/96
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface Vlan-interface300
ip address 192.168.3.3 255.255.255.0
ipv6 dhcp select server
ipv6 dhcp server apply pool 2
ipv6 address 3003::3/96
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 300
#
interface GigabitEthernet1/0/2
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 1 100 300
poe enable
#
return

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。

# 远程 Portal 认证热备典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                                  |    |
|----------------------------------|----|
| 1 简介.....                        | 1  |
| 2 配置前提 .....                     | 1  |
| 3 配置举例 .....                     | 1  |
| 3.1 组网需求 .....                   | 1  |
| 3.2 配置思路 .....                   | 2  |
| 3.3 配置注意事项 .....                 | 2  |
| 3.4 配置步骤 .....                   | 3  |
| 3.4.1 AC 1 的配置 .....             | 3  |
| 3.4.2 AC 2 的配置 .....             | 6  |
| 3.4.3 L3 switch 的配置 .....        | 9  |
| 3.4.4 L2 switch 的配置 .....        | 10 |
| 3.4.5 Portal/RADIUS 服务器的配置 ..... | 11 |
| 3.5 验证配置 .....                   | 18 |
| 3.6 配置文件 .....                   | 19 |
| 4 相关资料 .....                     | 23 |

# 1 简介

本文档介绍了远程 Portal 认证热备典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解远程 Portal 认证、双机热备、VRRP 和双 AC 备份等特性。

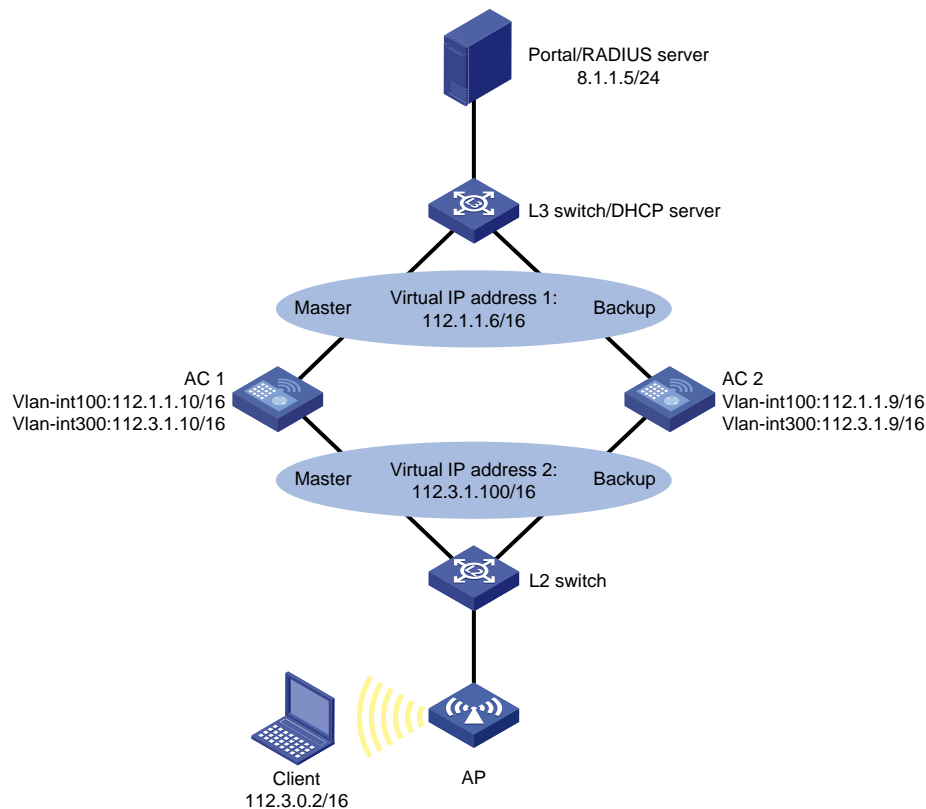
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，AC 1 和 AC 2 之间通过 VRRP 协议实现双机热备的流量切换，且两台设备均支持 Portal 认证功能。现要求 AC 1 和 AC 2 通过双机热备对 Portal 用户的业务信息进行备份。具体要求如下：

- AC 1 正常工作的情况下，Client 通过 AC 1 进行 Portal 认证接入。认证成功后在 AC 2 上能同时备份 Client 的 Portal 相关认证信息。
- 当 AC 1 发生故障时，Client 切换至 AC 2 上，保证业务流量切换不被中断。
- Portal/RADIUS 服务器作为认证/计费服务器，对 Client 进行远程 Portal 认证。
- AC1 和 AC2 通过 VLAN 100 传输双机热备报文，AC 1 和 AC 2 其中任何一条链路故障，将不会影响 Portal 用户数据转发。

图1 远程 Portal 认证热备组网图



## 3.2 配置思路

- 为了避免两台 AC 和下行设备 L2 switch 产生环路，并在主备切换时，尽快完成收敛，需要在 AC 1 和 AC 2 上使能 MSTP 功能，并设置 AC 1 为根桥。
- 为了实现 Portal 用户数据备份功能，需要分别在 AC 1 和 AC 2 上配置双 AC 备份功能，使 AC 1 和 AC 2 的用户数据同步。
- 为了实现互为备份的两台 AC 可以同时处理用户数据热备功能，需要分别在 AC 1 和 AC 2 上配置 VRRP 备份组，使 AC 1 和 AC 2 在同一 VRRP 组里。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 互为双机热备的两台 AC 对于 Portal 服务器和 AAA 服务器需要呈现同一个客户端 IP 地址，所以 AC 1 与 AC 2 配置的 Portal NAS-IP 必须为 VRRP 备份组 1 的虚拟 IP 地址。
- AC 1 与 AC 2 上与 Portal 和 WLAN 的相关配置必须一致。
- AC 1 与 AC 2 上所使用版本必须一致。
- AC 1 与 AC 2 配置 Nas Device-id 不能一致。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

#### (1) 配置 AC 1 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道，同时 VLAN 100 也作为业务备份 VLAN。

```
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 112.1.1.10 16
[AC1-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC1] vlan 200
[AC1-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC1] vlan 300
[AC1-vlan300] quit
```

# 配置 VLAN 300 的接口 IP 地址为 112.3.1.10/16。

```
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] ip address 112.3.1.10 16
[AC1-Vlan-interface300] quit
```

# 配置 AC 1 与 L2 switch 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC1-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC1-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS 1 接口，并设置端口的链路类型为 Hybrid。

```
[AC1] interface wlan-ess 1
[AC1-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。

```
[AC1-WLAN-ESS1] undo port hybrid vlan 1
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC1-WLAN-ESS1] mac-vlan enable
[AC1-WLAN-ESS1] quit
```

#### (2) 配置 MSTP

# 配置生成树的工作模式为 MSTP。

```
[AC1] stp mode mstp
```

# 激活 MST 域。

```
[AC1] stp region-configuration
[AC1-mst-region] active region-configuration
```

```

[AC1-mst-region] quit
# 配置 AC 1 为根桥。
[AC1] stp root primary
# 使能 STP 功能。
[AC1] stp enable
(3) 配置认证策略和认证域
# 在 AC 1 上创建 RADIUS 方案 office 并进入 RADIUS 方案视图。
<AC1> system-view
[AC1] radius scheme office
# 设置主认证、计费 RADIUS 服务器的 IP 地址为 8.1.1.5。
[AC1-radius-office] primary authentication 8.1.1.5
[AC1-radius-office] primary accounting 8.1.1.5
# 设置系统与认证、计费 RADIUS 服务器交互报文时的共享密钥为 123456789。
[AC1-radius-office] key authentication simple 123456789
[AC1-radius-office] key accounting simple 123456789
# 指定发送给 RADIUS 方案 office 中 RADIUS 服务器的用户名不得携带域名。
[AC1-radius-office] user-name-format without-domain
# 配置 RADIUS 方案中 NAS-IP 为 112.1.1.6。
[AC1-radius-office] nas-ip 112.1.1.6
[AC1-radius-office] quit
# 创建 office 域并进入其视图。
[AC1] domain office
# 在 ISP 域 office 下，为 Portal 用户配置认证、授权、计费方案为 RADIUS 方案，方案名为 office。
[AC1-isp-office] authentication portal radius-scheme office
[AC1-isp-office] authorization portal radius-scheme office
[AC1-isp-office] accounting portal radius-scheme office
# 设置当前 ISP 域下的用户闲置切断功能，闲置检测时间为 60 分钟。
[AC1-isp-office] idle-cut enable 60
[AC1-isp-office] quit
(4) 配置 Portal Server
# 配置 Portal 服务器 portal 的 IP 地址为 8.1.1.5、密钥为明文 123456789、HTTP 重定向的 URL 为
http://8.1.1.5:8080/portal。
[AC1] portal server portal ip 8.1.1.5 key simple 123456789 url http://8.1.1.5:8080/portal
# 配置在接口 VLAN 300 上启用 Portal 认证，并配置为直接认证方式。
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] portal server portal method direct
# 配置从接口 VLAN 300 接入的 IPv4 Portal 用户使用认证域为 office。
[AC1-Vlan-interface300] portal domain office
# 配置双机热备组网环境中，Master AC 的业务备份接口 VLAN 300 属于 Portal 备份组 1。
[AC1-Vlan-interface300] portal backup-group 1
# 配置接口 VLAN 300 发送 Portal 报文使用的 IPv4 源地址为 112.1.1.6。
[AC1-Vlan-interface300] portal nas-ip 112.1.1.6
[AC1-Vlan-interface300] quit
# 配置双机热备模式下的设备 ID 为 1。

```

```

[AC1] nas device-id 1
# 使能双机热备业务备份功能，且支持对称路径。
[AC1] dnbk enable backup-type symmetric-path
# 配置双机热备业务备份 VLAN 为 VLAN 100。
[AC1] dnbk vlan 100
# 配置 Portal 免认证规则，使得符合源接口为 AC 1 与 L2 switch 相连的接口的报文不会触发 Portal 认证。
[AC1] portal free-rule 0 source interface gigabitethernet 1/0/1
(5) 配置到 Portal/Radius 服务器的静态路由
# 配置下一跳地址为 L3 switch 的 VLAN 100 接口地址的静态路由。
[AC1] ip route-static 8.0.0.0 255.0.0.0 112.1.1.5
(6) 配置 AC 1 的 WLAN 双机热备
# 配置 AC 1 的备份 AC，即 AC 2 的 IP 地址为 112.1.1.9。
[AC1] wlan backup-ac ip 112.1.1.9
# 使能 AC 1 的热备份功能。
[AC1] hot-backup enable
# 配置 AC 1 用于热备份的本端数据端口的 VLAN ID 为 200。
[AC1] hot-backup vlan 200
(7) 配置 VRRP 功能
# 配置 AC 1 的 VLAN 100 接口加入 VRRP 备份组 1，VRRP 备份组 1 的虚拟 IP 地址为 112.1.1.6。
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] vrrp vrid 1 virtual-ip 112.1.1.6
# 配置备份组优先级为 250，以保证 AC 1 成为 VRRP 组 1 的 Master 设备。
[AC1-Vlan-interface100] vrrp vrid 1 priority 250
[AC1-Vlan-interface100] quit
# 配置 AC 1 的 VLAN 300 接口加入 VRRP 备份组 2，VRRP 备份组 2 的虚拟 IP 地址为 112.3.1.100。
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] vrrp vrid 2 virtual-ip 112.3.1.100
# 配置备份组优先级为 250，以保证 AC 1 成为 VRRP 组 2 的 Master 设备。
[AC1-Vlan-interface300] vrrp vrid 2 priority 250
[AC1-Vlan-interface300] quit
(8) 配置无线服务
# 创建 clear 类型的服务模板 1。
[AC1] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service。
[AC1-wlan-st-1] ssid service
# 将 WLAN-ESS 1 接口绑定到服务模板 1。
[AC1-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
(9) 配置射频接口并绑定服务模板
# 创建 AP 的管理模板，名称为 officeap，型号名称这里选择 WA2620E-AGN。

```



```

[AC1] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC1-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC1-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN
为 VLAN 300。
[AC1-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC1-wlan-ap-officeap-radio-2] radio enable
[AC1-wlan-ap-officeap-radio-2] quit

```

### 3.4.2 AC 2 的配置

#### (1) 配置 AC 2 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```

[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 112.1.1.9 16
[AC2-Vlan-interface100] quit

```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```

[AC2] vlan 200
[AC2-vlan200] quit

```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```

[AC2] vlan 300
[AC2-vlan300] quit

```

# 配置 VLAN 300 的接口 IP 地址为 112.3.1.9/16。

```

[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] ip address 112.3.1.9 16
[AC2-Vlan-interface300] quit

```

# 配置 AC 2 与 L2 switch 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```

[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC2-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC2-GigabitEthernet1/0/1] quit

```

# 创建 WLAN-ESS 1 接口，并设置端口的链路类型为 Hybrid。

```

[AC2] interface wlan-ess 1
[AC2-WLAN-ESS1] port link-type hybrid

```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。

```

[AC2-WLAN-ESS1] undo port hybrid vlan 1
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged

```

```
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC2-WLAN-ESS1] mac-vlan enable
```

```
[AC2-WLAN-ESS1] quit
```

## (2) 配置 MSTP

# 配置生成树的工作模式为 MSTP。

```
[AC2] stp mode mstp
```

# 激活 MST 域。

```
[AC2] stp region-configuration
```

```
[AC2-mst-region] active region-configuration
```

```
[AC2-mst-region] quit
```

# 使能 STP 功能。

```
[AC2] stp enable
```

## (3) 配置认证策略和认证域

# 在 AC 2 上创建 RADIUS 方案 office 并进入其视图。

```
<AC2> system-view
```

```
[AC2] radius scheme office
```

# 设置主认证、计费 RADIUS 服务器的 IP 地址为 8.1.1.5。

```
[AC2-radius-office] primary authentication 8.1.1.5
```

```
[AC2-radius-office] primary accounting 8.1.1.5
```

# 设置系统与认证、计费 RADIUS 服务器交互报文时的共享密钥为 123456789。

```
[AC2-radius-office] key authentication simple 123456789
```

```
[AC2-radius-office] key accounting simple 123456789
```

# 指定发送给 RADIUS 方案 office 中 RADIUS 服务器的用户名不得携带域名。

```
[AC2-radius-office] user-name-format without-domain
```

# 配置 RADIUS 方案中 NAS-IP 为 112.1.1.6。

```
[AC2-radius-office] nas-ip 112.1.1.6
```

```
[AC2-radius-office] quit
```

# 创建 office 域并进入其视图。

```
[AC2] domain office
```

# 在 ISP 域 office 下，为 Portal 用户配置认证、授权、计费方案为 RADIUS 方案，方案名为 office。

```
[AC2-isp-office] authentication portal radius-scheme office
```

```
[AC2-isp-office] authorization portal radius-scheme office
```

```
[AC2-isp-office] accounting portal radius-scheme office
```

# 设置当前 ISP 域下的用户闲置切断功能，闲置检测时间为 60 分钟。

```
[AC2-isp-office] idle-cut enable 60
```

```
[AC2-isp-office] quit
```

## (4) 配置 Portal Server

# 配置 Portal 服务器 portal 的 IP 地址为 8.1.1.5、密钥为明文 123456789、HTTP 重定向的 URL 为 http://8.1.1.5:8080/portal。

```
[AC2] portal server portal ip 8.1.1.5 key simple 123456789 url http://8.1.1.5:8080/portal
```

# 配置在接口 VLAN 300 上启用三层 Portal 认证，并配置为直接认证方式。

```
[AC2] interface vlan-interface 300
```

```
[AC2-Vlan-interface300] portal server portal method direct
```

```

# 配置从接口 VLAN 300 接入的 IPv4 Portal 用户使用认证域为 office。
[AC2-Vlan-interface300] portal domain office
# 配置双机热备组网环境中，BackupAC 的业务备份接口 VLAN 300 属于 Portal 备份组 1。
[AC2-Vlan-interface300] portal backup-group 1
# 配置接口 VLAN 300 发送 Portal 报文使用的 IPv4 源地址为 112.1.1.6。
[AC2-Vlan-interface300] portal nas-ip 112.1.1.6
[AC2-Vlan-interface300] quit
# 配置双机热备模式下的设备 ID 为 2。
[AC2] nas device-id 2
# 使能双机热备业务备份功能，且支持对称路径。
[AC2] dnbk enable backup-type symmetric-path
# 配置双机热备业务备份 VLAN 为 VLAN 100。
[AC2] dnbk vlan 100
# 配置 Portal 免认证规则，使得符合源接口为 AC 2 与 L2 switch 相连的接口的报文不会触发 Portal 认证。
[AC2] portal free-rule 0 source interface gigabitethernet 1/0/1
(5) 配置到 Portal/Radius 服务器的静态路由
# 配置下一跳地址为 L3 switch 的 VLAN 100 接口地址的静态路由
[AC2] ip route-static 8.0.0.0 255.0.0.0 112.1.1.5
(6) 配置 AC 2 的双 AC 备份功能
# 配置 AC 2 的备份 AC，即 AC 1 的 IP 地址为 112.1.1.10。
[AC2] wlan backup-ac ip 112.1.1.10
# 使能 AC 2 的热备份功能。
[AC2] hot-backup enable
# 配置 AC 2 用于热备份的本端数据端口的 VLAN ID 为 200。
[AC2] hot-backup vlan 200
(7) 配置 VRRP 功能
# 配置 AC 2 的 VLAN 100 接口加入 VRRP 备份组 1，虚拟 IP 地址为 112.1.1.6，AC 2 在备份组 1 中的优先级取缺省值 100。
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] vrrp vrid 1 virtual-ip 112.1.1.6
[AC2-Vlan-interface100] quit
# 配置 AC 2 的 VLAN 300 接口加入 VRRP 备份组 2，虚拟 IP 地址为 112.3.1.100，AC 2 在备份组 2 中的优先级取缺省值 100。
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] vrrp vrid 2 virtual-ip 112.3.1.100
[AC2-Vlan-interface300] quit
(8) 配置无线服务
# 创建 clear 类型的服务模板 1。
[AC2] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service。
[AC2-wlan-st-1] ssid service
# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```

```

[AC2-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
(9) 配置射频接口并绑定服务模板
# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。
[AC2] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC2-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC2-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN
为 VLAN 300。
[AC2-wlan-ap-officeap1-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC2-wlan-ap-officeap1-radio-2] radio enable
[AC2-wlan-ap-officeap1-radio-2] quit

```

### 3.4.3 L3 switch 的配置

```

# 创建 VLAN 100 和 VLAN 300。
<L3 switch> system-view
[L3 switch] vlan 100
[L3 switch-vlan100] quit
[L3 switch] vlan 300
[L3 switch-vlan300] quit
# 配置 VLAN 100 接口的 IP 地址为 112.1.1.5/16，作为 AC 到 Portal/Radius 服务器的静态路由的下一跳。
[L3 switch] interface vlan-interface 300
[L3 switch-Vlan-interface100] ip address 112.1.1.5 16
[L3 switch-Vlan-interface100] quit
# 配置 L3 switch 使能 DHCP 服务。
[L3 switch] dhcp enable
# 创建名为 vlan100 的 DHCP 地址池，配置动态分配的网段为 112.1.0.0/16，网关地址为 112.1.1.6，
为 AP 分配 IP 地址。
[L3 switch] dhcp server ip-pool vlan100
[L3 switch-dhcp-pool-vlan100] network 112.1.0.0 mask 255.255.0.0
[L3 switch-dhcp-pool-vlan100] gateway-list 112.1.1.6
[L3 switch-dhcp-pool-vlan100] quit
# 创建名为 vlan300 的 DHCP 地址池，配置动态分配的网段为 112.3.0.0/16，网关地址为 112.3.1.100，
为 Client 分配 IP 地址。
[L3 switch] dhcp server ip-pool vlan300
[L3 switch-dhcp-pool-vlan300] network 112.3.0.0 mask 255.255.0.0
[L3 switch-dhcp-pool-vlan300] gateway-list 112.3.1.100
[L3 switch-dhcp-pool-vlan300] quit

```

### 3.4.4 L2 switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线用户接入的 VLAN。

```
<L2 switch> system-view
[L2 switch] vlan 100
[L2 switch-vlan100] quit
[L2 switch] vlan 300
[L2 switch-vlan300] quit
```

# 配置 Switch 与 AC 1 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk, PVID 为 100, 并允许 VLAN 100 和 VLAN 300 通过。

```
[L2 switch] interface gigabitethernet 1/0/1
[L2 switch-GigabitEthernet1/0/1] port link-type trunk
[L2 switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[L2 switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[L2 switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access, 并允许 VLAN 100 通过, 并使能 PoE 功能。

```
[L2 switch] interface gigabitethernet 1/0/2
[L2 switch-GigabitEthernet1/0/2] port link-type access
[L2 switch-GigabitEthernet1/0/2] port access vlan 100
[L2 switch-GigabitEthernet1/0/2] poe enable
[L2 switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AC 2 相连的 GigabitEthernet1/0/3 接口的链路类型为 Trunk, PVID 为 100, 并允许 VLAN 100 和 VLAN 300 通过。

```
[L2 switch] interface gigabitethernet 1/0/3
[L2 switch-GigabitEthernet1/0/3] port link-type trunk
[L2 switch-GigabitEthernet1/0/3] port trunk permit vlan 100 300
[L2 switch-GigabitEthernet1/0/3] port trunk pvid vlan 100
[L2 switch-GigabitEthernet1/0/3] quit
```

# 配置生成树的工作模式为 MSTP。

```
[L2 switch] stp mode mstp
```

# 激活 MST 域。

```
[L2 switch] stp region-configuration
[L2 switch-mst-region] active region-configuration
[L2 switch-mst-region] quit
```

# 使能 STP 功能。

```
[L2 switch] stp enable
```

### 3.4.5 Portal/RADIUS 服务器的配置



说明

下面以 IMC 为例(使用 IMC 版本为: iMC PLAT 7.0 (E0202)、iMC WSM 7.0 (E0202) ), 说明 Portal server、Radius Server 的基本配置。

#### # 增加接入设备

登录进入 IMC 管理平台, 选择“用户”页签, 单击导航树中的[接入设备管理/接入设备配置/接入设备配置]菜单项, 进入“接入设备配置”页面, 在该页面中单击<增加>按钮, 进入“增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456789”;
- 设置认证及计费的端口号分别为“1812”和“1813”;
- 选择业务类型为“LAN 接入业务”;
- 选择接入设备类型为“H3C(General)”;
- 在设备列表中, 单击<手工增加>按钮, 添加 IP 地址为 112.1.1.6 的接入设备;
- 其它参数采用缺省值, 并单击<确定>按钮完成操作。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \* 1812

计费端口 \* 1813

组网方式 不启用混合组网

业务类型 LAN接入业务

接入设备类型 H3C(General)

接入设备分组 无

共享密钥 \* .....

确认共享密钥 \* .....

业务分组 未分组

设备列表

选择 手工增加 全部清除

| 设备名称 | 设备IP地址    | 设备型号 | 备注 | 删除 |
|------|-----------|------|----|----|
|      | 112.1.1.6 |      |    | 删除 |

共有1条记录。

确定 取消

#### # 增加接入策略。

选择“用户”页签, 单击导航树中的[接入策略管理/接入策略管理]菜单项, 进入“接入策略管理”页面, 单击<增加>按钮, 进入“增加接入策略”页面。

- 接入策略名为“portal”, 该名称可以自行定义;
- 业务分组选择“未分组”;
- 其它参数采用缺省值, 并单击<确定>按钮完成操作。

图3 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略 帮助

基本信息

接入策略名 \*

portal

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☒ 不启用 ☐ EAP证书认证 ☐ WAP证书认证

认证证书类型

EAP-TLS认证

下发VLAN

☐ 下发User Profile

下发用户组

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Windows可溶解客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔(分钟) 30

自动重连次数 3

违规处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式

☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定

取消

# 增加接入服务配置。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入“接入服务管理”页面，在该页面中单击<增加>按钮，进入“增加接入服务”页面。

- 输入服务名“portal auth”，该名称可以自行定义；
- 业务分组“未分组”；
- 缺省接入策略“portal”，即上一步配置的接入策略名；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 ? 帮助

基本信息

服务名 \*

portal auth

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

802.1x

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 (PC)

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“admin”；
- 输入证件号码“12345”；
- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图5 增加用户

增加用户

基本信息

用户姓名 \*

admin

证件号码 \*

12345

检查是否可用

通讯地址

电话

电子邮件

用户分组 \*

未分组

确定

取消

在“增加接入用户”页面，按如下方式配置。

- 输入账号名“user”；
- 输入密码“123456”；



- 接入服务选择 “portal auth” ；
- 其他配置保持默认；
- 单击<确定>按钮完成操作。

图6 增加接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

admin

选择

增加用户

帐号名 \*

user

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数里限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                             | 服务后缀 | 状态      | 分配IP地址 |
|-------------------------------------------------|------|---------|--------|
| <input checked="" type="checkbox"/> portal auth |      | 可申<br>请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线SSID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

IP地址

MAC地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

# 配置 Portal 主页

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入“服务器配置”页面，配置 Portal 主页，采用默认配置即可，单击<确定>按钮完成。

图7 服务器配置

用户 > 接入策略管理 > Portal服务管理 > 服务器配置

帮助

Portal服务器配置

基本信息

日志级别 \*

信息

Portal Server

报文请求超时时长(秒) \*

4

逃生心跳间隔时长(秒) \*

20

用户心跳间隔时长(分钟) \*

5

Portal Web

请求报文超时时长(秒) \*

15

交互报文编码

校验终端用户请求报文

是

使用缓存

是

HTTP心跳界面展示方式

新页面

HTTPS心跳界面展示方式

原页面

Portal主页

http://8.1.15:8080/portal/

高级信息

服务类型列表

增加

共有0条记录。

服务类型标识

服务类型

删除

未找到符合条件的记录。

确定

# 配置 Portal 认证的地址组范围

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，单击<增加>按钮，配置 Portal 认证的地址组范围。

- 配置 IP 地址组名为“portal”；
- 配置起始地址为 112.3.0.0；
- 配置终止地址为 112.3.255.255；
- 其他采用默认配置；
- 单击<确定>按钮完成操作。

16

图8 增加 IP 地址组

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组 帮助

增加IP地址组

IP地址组名 \*

portal

起始地址 \*

112.3.0.0

终止地址 \*

112.3.255.255

业务分组

未分组

类型 \*

普通

确定

取消

# 配置接入设备信息

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，单击“增加”按钮，配置 Portal 认证的接入设备。

- 配置设备名为“AC”；
- 配置 IP 地址为 112.1.1.6；
- 配置密钥为“123456789”，该密钥与 AC 上配置 Portal 服务器时设置的密钥一致；
- 其他采用默认配置即可；
- 单击<确定>按钮完成操作。

图9 增加设备信息

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息 帮助

增加设备信息

设备信息

设备名 \*

AC

版本 \*

Portal 2.0

监听端口 \*

2000

认证重发次数 \*

0

支持逃生心跳 \*

否

密钥 \*

.....

组网方式 \*

三层

设备描述

业务分组 \*

未分组

IP地址 \*

112.1.1.6

本地Challenge \*

否

下线重发次数 \*

1

支持用户心跳 \*

否

确认密钥 \*

.....

确定

取消

# 配置端口组


返回[用户接入管理/Portal 服务管理/设备配置]菜单项，在“设备信息列表”中找到设备 AC，在“操作”列表下选中<端口组信息管理>按钮，图标为，进入“端口组信息配置”页签。

图10 设备配置

用户 > 接入策略管理 > Portal服务管理 > 设备配置 ★加入收藏 ?帮助

设备信息查询

设备名  版本

下发结果  业务分组  查询 重置

增加

| 设备名 | 版本         | 业务分组 | IP地址      | 最近一次下发时间 | 下发结果 | 操作 |
|-----|------------|------|-----------|----------|------|----|
| AC  | Portal 2.0 | 未分组  | 112.1.1.6 |          | 未下发  |    |

共有1条记录, 当前第1-1, 第 1/1 页。

1 50

在“端口组信息列表”子页签，单击<增加>按钮，进入到“增加端口组信息”页面。

- 配置端口组名为“port\_portal”；
- 配置 IP 地址组，选取创建的地址组“portal”；
- 其他采用默认配置即可；
- 单击<确定>按钮完成操作。

图11 增加端口组信息

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 增加端口组信息 ?帮助

增加端口组信息

|            |                                          |            |                                     |
|------------|------------------------------------------|------------|-------------------------------------|
| 端口组名 *     | <input type="text" value="port_portal"/> | 提示语言 *     | <input type="text" value="动态检测"/>   |
| 开始端口 *     | <input type="text" value="0"/>           | 终止端口 *     | <input type="text" value="255"/>    |
| 协议类型 *     | <input type="text" value="HTTP"/>        | 快速认证 *     | <input type="text" value="否"/>      |
| 是否NAT *    | <input type="text" value="否"/>           | 错误透传 *     | <input type="text" value="是"/>      |
| 认证方式 *     | <input type="text" value="CHAP认证"/>      | IP地址组 *    | <input type="text" value="portal"/> |
| 心跳间隔(分钟) * | <input type="text" value="10"/>          | 心跳超时(分钟) * | <input type="text" value="30"/>     |
| 用户域名       | <input type="text"/>                     | 端口组描述      | <input type="text"/>                |
| 无感知认证      | <input type="text" value="不支持"/>         | 客户端防破解 *   | <input type="text" value="否"/>      |
| 用户属性类型     | <input type="text"/>                     | 缺省认证页面     | <input type="text"/>                |

确定 取消

### 3.5 验证配置

# Client 从 AC 1 成功上线后,在 AC 1 上通过命令 **display portal user all** 查看该用户的认证情况。可以看到 Portal 用户的工作模式为主用户模式 **primary**，表示该用户是由 AC 1 上线。

```
[AC1] display portal user all
Index:0
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:primary
MAC          IP          Vlan  Interface
```

```
-----
3ca9-f414-4c20 112.3.0.2 300 Vlan-interface300
```

```
Total 1 user(s) matched, 1 listed.
```

# Client 从 AC 1 成功上线后，在 AC 2 通过命令 **display portal user all** 查看该用户的认证情况。可以看到 Portal 用户的工作模式为备用户模式 **secondary**，表示该用户的认证信息同步到 AC 2 上。

```
[AC2] display portal user all
```

```
Index:0
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode:secondary
```

```
MAC IP Vlan Interface
```

```
-----
3ca9-f414-4c20 112.3.0.2 300 Vlan-interface300
```

```
Total 1 user(s) matched, 1 listed.
```

# 通过将 AC 1 下电模拟主 AC 宕机的情形，使得 AC 发生主备切换，此时，在 AC 2 上便可以查看到用户的状态由“secondary”转换为“stand-alone”状态，说明此时只有 AC 2 处于工作状态。

```
[AC2] display portal user all
```

```
Index:0
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode:stand-alone
```

```
MAC IP Vlan Interface
```

```
-----
3ca9-f414-4c20 112.3.0.2 300 Vlan-interface300
```

```
Total 1 user(s) matched, 1 listed.
```

## 3.6 配置文件

- AC 1 的配置文件：

```
#
```

```
portal server portal ip 8.1.1.5 key cipher $c$3$yPJYbIZntOml+Mp2097juefT3q3lvkuGWoqXWw== url  
http://8.1.1.5:8080/portal
```

```
portal free-rule 1 source interface GigabitEthernet1/0/1 destination any
```

```
#
```

```
wlan backup-ac ip 112.1.1.9
```

```
#
```

```
hot-backup enable domain 1
```

```
hot-backup vlan 200
```

```
#
```

```
vlan 100
```

```
#
```

```
vlan 200
```

```
#
```

```
vlan 300
```

```
#
```

```
stp instance 0 root primary
```

```

stp enable
#
radius scheme office
    primary authentication 8.1.1.5
    primary accounting 8.1.1.5
key authentication cipher $c$3$Vy4zlTRK9dGfqIRznkpunGreP66fzGClKx+/3w==
key accounting cipher $c$3$FNRuWQMfrvaCHSE8tgxhQtnuUSaGAScmBCWdDA==
    user-name-format without-domain
    nas-ip 112.1.1.6
#
domain office
    authentication portal radius-scheme office
    authorization portal radius-scheme office
    accounting portal radius-scheme office
    access-limit disable
    state active
    idle-cut enable 60 10240
    self-service-url disable
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
interface Vlan-interface100
    ip address 112.1.1.10 255.255.0.0
    vrrp vrid 1 virtual-ip 112.1.1.6
    vrrp vrid 1 priority 250
#
interface Vlan-interface300
    ip address 112.3.1.10 255.255.0.0
    vrrp vrid 2 virtual-ip 112.3.1.100
    vrrp vrid 2 priority 250
    portal server portal method direct
    portal domain office
    portal backup-group 1
    portal nas-ip 112.1.1.6
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 300
    port trunk pvid vlan 100
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200

```

```

mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
    serial-id 21023529G007C000020
    radio 1
    radio 2
    service-template 1 vlan-id 300
    radio enable
#
ip route-static 8.0.0.0 255.0.0.0 112.1.1.5
#
dwbk enable backup-type symmetric-path
dwbk vlan 100
#
•   AC 2 的配置文件:
#
port-security enable
#
portal server portal ip 8.1.1.5 key cipher $c$3$qWCKr5ioUOEhJeHSVPpx7VceW+Y9tR
ss6aDRkQ== url http://8.1.1.5:8080/portal
portal free-rule 1 source interface GigabitEthernet1/0/1 destination any
#
wlan backup-ac ip 112.1.1.10
#
hot-backup enable domain 1
hot-backup vlan 200
#
vlan 100
#
vlan 200
#
vlan 300
#
stp enable
#
radius scheme office
    primary authentication 8.1.1.5
    primary accounting 8.1.1.5
    key authentication cipher $c$3$DwdyO3FJaT6fUII3MkEHQ8OLzb5+8KT3Bhk3Og==
    key accounting cipher $c$3$nVZDWB52/+OctKvssb6qF8o3X5B3slIcrDrnKQ==
    user-name-format without-domain
    nas-ip 112.1.1.6
#
domain office
    authentication portal radius-scheme office
    authorization portal radius-scheme office
    accounting portal radius-scheme office
    access-limit disable

```



```

state active
idle-cut enable 60 10240
self-service-url disable
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 112.1.1.9 255.255.0.0
vrrp vrid 1 virtual-ip 112.1.1.6
#
interface Vlan-interface300
ip address 112.3.1.9 255.255.0.0
vrrp vrid 2 virtual-ip 112.3.1.100
portal server portal method direct
portal domain office
portal backup-group 1
portal nas-ip 112.1.1.6
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap office model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1 vlan-id 300
radio enable
#
ip route-static 8.0.0.0 255.0.0.0 112.1.1.5
#
dhbk enable backup-type symmetric-path
dhbk vlan 100
#

```

- L3 Switch 的配置文件:

```

#
vlan 100

```

```
#
vlan 300
#
interface Vlan-interface300
ip address 112.1.1.5 255.255.0.0
#
dhcp enable
#
dhcp server ip-pool vlan100
network 112.1.0.0 mask 255.255.0.0
gateway-list 112.1.1.6
#
dhcp server ip-pool vlan300
network 112.3.0.0 mask 255.255.0.0
gateway-list 112.3.1.100
#
```

- L2 Switch 的配置文件：

```
#
vlan 100
#
vlan 300
#
stp enable
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。

- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“可靠性配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“可靠性命令参考”。

# 远程 IPv6 Portal 认证热备典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                                  |    |
|----------------------------------|----|
| 1 简介.....                        | 1  |
| 2 配置前提 .....                     | 1  |
| 3 配置举例 .....                     | 1  |
| 3.1 组网需求 .....                   | 1  |
| 3.2 配置思路 .....                   | 2  |
| 3.3 配置注意事项.....                  | 2  |
| 3.4 配置步骤 .....                   | 3  |
| 3.4.1 AC 1 的配置 .....             | 3  |
| 3.4.2 AC 2 的配置 .....             | 7  |
| 3.4.3 Switch 1 的配置 .....         | 12 |
| 3.4.4 Switch 2 的配置 .....         | 12 |
| 3.4.5 Portal/RADIUS 服务器的配置 ..... | 13 |
| 3.5 验证配置 .....                   | 20 |
| 3.6 配置文件 .....                   | 21 |
| 4 相关资料 .....                     | 28 |

# 1 简介

本文档介绍了远程 Portal 认证热备典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解远程 Portal 认证、双机热备、VRRP 和双 AC 备份等特性。

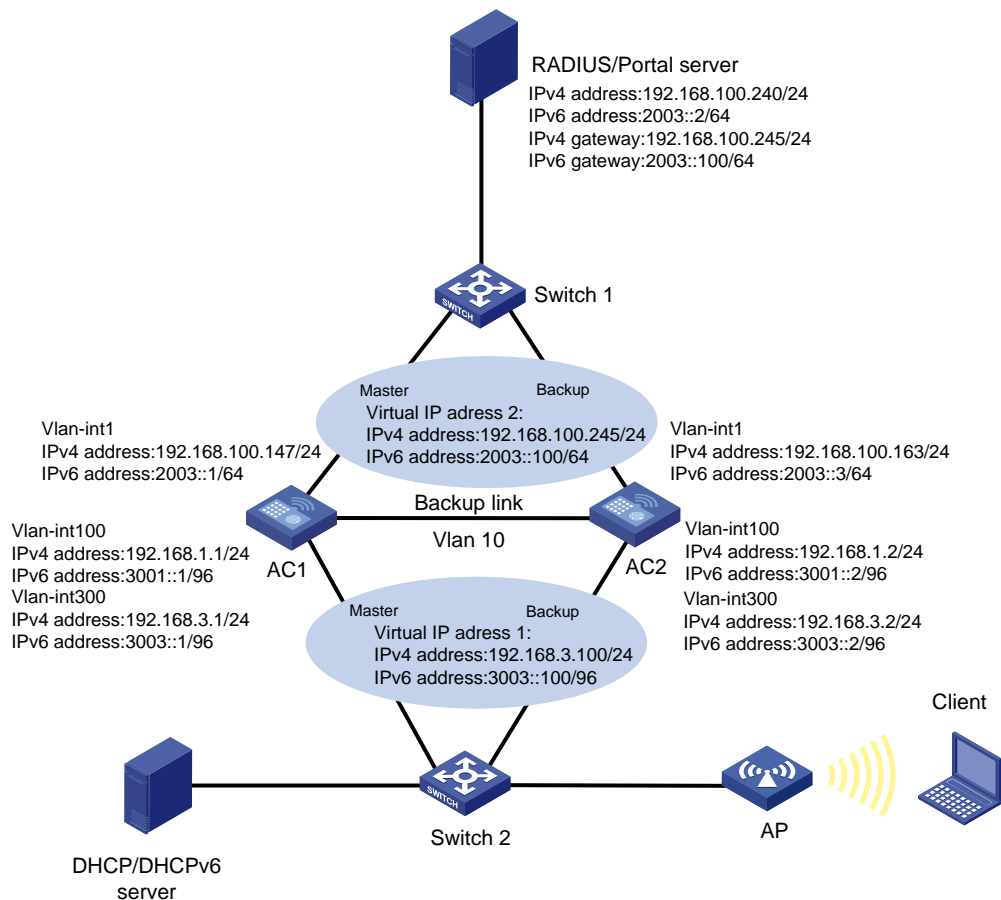
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，AC 1 和 AC 2 之间通过 VRRP 协议实现双机热备的流量切换，且两台设备均支持 Portal 认证功能。现要求 AC 1 和 AC 2 通过双机热备对 Portal 用户的业务信息进行备份。具体要求如下：

- AC 1 正常工作的情况下，Client 通过 AC 1 进行 Portal 认证接入。认证成功后在 AC 2 上能同时备份 Client 的 Portal 相关认证信息。
- 当 AC 1 发生故障时，Client 切换至 AC 2 上，保证业务流量切换不被中断。
- Portal/RADIUS 服务器作为认证/计费服务器，对 Client 进行远程 Portal 认证。
- AC1 和 AC2 通过 VLAN 10 传输双机热备报文。

图1 远程 Portal 认证热备组网图



## 3.2 配置思路

- 为了避免两台 AC 和上下行设备产生环路，并在主备切换时，尽快完成收敛，需要在 AC 1 和 AC 2 上使能 MSTP 功能，并设置 AC 1 为根桥。
- 为了实现 Portal 用户数据备份功能，需要分别在 AC 1 和 AC 2 上配置双 AC 备份功能，使 AC 1 和 AC 2 的用户数据同步。
- 为了实现互为备份的两台 AC 可以同时处理用户数据热备功能，需要分别在 AC 1 和 AC 2 上配置 VRRP 备份组，使 AC 1 和 AC 2 在同一 VRRP 组里。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 互为双机热备的两台 AC 对于 Portal 服务器和 AAA 服务器需要呈现同一个客户端 IP 地址，所以 AC 1 与 AC 2 配置的 Portal NAS-IP 必须为 VRRP 备份组 1 的虚拟 IP 地址。
- AC 1 与 AC 2 上 Portal 和 WLAN 的相关配置必须一致。
- AC 1 与 AC 2 上所使用版本必须一致。
- AC 1 与 AC 2 配置 Nas Device-id 不能一致。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

#### (1) 配置 AC 1 的接口

# 全局使能 IPv6 功能。

```
<AC1> system-view
```

```
[AC1] ipv6
```

# 创建 VLAN 10 作为双机热备的 VLAN。

```
[AC1] vlan 10
```

```
[AC1-vlan10] quit
```

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv4 和 IPv6 地址。AP 将通过该 VLAN 与 AC 建立 LWAPP 隧道。

```
[AC1] vlan 100
```

```
[AC1-vlan100] quit
```

```
[AC1] interface vlan-interface 100
```

```
[AC1-Vlan-interface100] ip address 192.168.1.1 24
```

```
[AC1-Vlan-interface100] ipv6 address 3001::1 96
```

```
[AC1-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC1] vlan 200
```

```
[AC1-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IPv4 和 IPv6 地址。

```
[AC1] vlan 300
```

```
[AC1-vlan300] quit
```

```
[AC1] interface vlan-interface 300
```

```
[AC1-Vlan-interface300] ip address 192.168.3.1 24
```

```
[AC1-Vlan-interface300] ipv6 address fe80::1 link-local
```

```
[AC1-Vlan-interface300] ipv6 address 3003::1 96
```

```
[AC1-Vlan-interface300] quit
```

# 创建 VLAN 1 作为与 RADIUS server 通信的 VLAN，并为该接口配置 IPv4 和 IPv6 地址。

```
[AC1] vlan 1
```

```
[AC1-vlan1] quit
```

```
[AC1] interface vlan-interface 1
```

```
[AC1-Vlan-interface1] ip address 192.168.100.147 24
```

```
[AC1-Vlan-interface1] ipv6 address fe80::2 link-local
```

```
[AC1-Vlan-interface1] ipv6 address 2003::1 64
```

```
[AC1-Vlan-interface1] quit
```

# 配置 AC 1 与 AC 2 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access，当前 Access 口允许 VLAN 10 通过。

```
[AC1] interface gigabitethernet 1/0/2
```

```
[AC1-GigabitEthernet1/0/2] port link-type access
```

```
[AC1-GigabitEthernet1/0/2] port access vlan 10
```

```
[AC1-GigabitEthernet1/0/2] quit
```

# 配置 AC1 的下行链路 GigabitEthernet1/0/3 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，并允许 VLAN 100 和 VLAN 300 的报文通过。



```
[AC1] interface gigabitethernet 1/0/3
[AC1-GigabitEthernet1/0/3] port link-type trunk
[AC1-GigabitEthernet1/0/3] port trunk permit vlan 100 300
[AC1-GigabitEthernet1/0/3] port trunk pvid vlan 100
[AC1-GigabitEthernet1/0/3] quit
```

## (2) 配置 MSTP

# 配置生成树的工作模式为 MSTP。

```
[AC1] stp mode mstp
# 激活 MST 域。
[AC1] stp region-configuration
[AC1-mst-region] active region-configuration
[AC1-mst-region] quit
```

# 配置 AC 1 为根桥。

```
[AC1] stp root primary
```

# 使能 STP 功能。

```
[AC1] stp enable
```

## (3) 配置 VRRP

# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IPv4 地址为 192.168.3.100，虚拟 IPv6 地址为 FE80::30 和 3003::100。

```
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] vrrp vrid 1 virtual-ip 192.168.3.100
[AC1-Vlan-interface300] vrrp ipv6 vrid 1 virtual-ip fe80::30 link-local
[AC1-Vlan-interface300] vrrp ipv6 vrid 1 virtual-ip 3003::100
```

# 配置 VLAN 接口 300 在 VRRP 备份组 1 中的优先级为 254。

```
[AC1-Vlan-interface300] vrrp vrid 1 priority 254
[AC1-Vlan-interface300] vrrp ipv6 vrid 1 priority 254
[AC1-Vlan-interface300] quit
```

# 创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IPv4 地址为 192.168.100.245，虚拟 IPv6 地址为 FE80::40 和 2003::100。

```
[AC1] interface vlan-interface 1
[AC1-Vlan-interface1] vrrp vrid 2 virtual-ip 192.168.100.245
[AC1-Vlan-interface1] vrrp ipv6 vrid 2 virtual-ip fe80::40 link-local
[AC1-Vlan-interface1] vrrp ipv6 vrid 2 virtual-ip 2003::100
```

# 配置 VLAN 接口 1 在 VRRP 备份组 2 中的优先级为 254。

```
[AC1-Vlan-interface1] vrrp vrid 2 priority 254
[AC1-Vlan-interface1] vrrp ipv6 vrid 2 priority 254
[AC1-Vlan-interface400] quit
```

## (4) 配置 Portal 认证

# 配置 IPv4 Portal 服务器：名称为 officev4，IPv4 地址为 192.168.100.240、密钥为明文 123456789，URL 为 http://192.168.100.240:8080/portal。

```
[AC1] portal server officev4 ip 192.168.100.240 key simple 123456789 url
http://192.168.100.240:8080/portal
```

# 配置 IPv6 Portal 服务器：名称为 officev6，IPv6 地址为 2003::2。

```
[AC1] portal server officev6 ipv6 2003::2 key simple 123456789 url
http://[2003::2]:8080/portal
```

# 在 VLAN 接口 300 上配置 Portal 用户报文的控制模式为 MAC，IPv4 或者 IPv6 用户通过 Portal 认证上线后，同时允许该用户的 IPv4 和 IPv6 报文通过认证接口。

```
[AC1] interface vlan-interface 300
```

```
[AC1-Vlan-interface300] portal control-mode mac
```

# 在 VLAN 接口 300 上使能 Portal 认证，并配置为直接认证方式。

```
[AC1-Vlan-interface300] portal server officev4 method direct
```

```
[AC1-Vlan-interface300] portal server officev6 method direct
```

```
[AC1-Vlan-interface300] quit
```

#### (5) 配置 IPv4 RADIUS 方案

# 创建名为 rs4 的 RADIUS 方案并进入其视图。

```
[AC1] radius scheme rs4
```

# 配置 RADIUS 方案的主认证服务器的 IPv4 地址为 192.168.100.240，认证报文的共享密钥设置为明文 123456。

```
[AC1-radius-rs4] primary authentication 192.168.100.240
```

```
[AC1-radius-rs4] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC1-radius-rs4] user-name-format without-domain
```

```
[AC1-radius-rs4] quit
```

#### (6) 配置 IPv6 RADIUS 方案

# 创建名为 rs6 的 RADIUS 方案并进入其视图。

```
[AC1] radius scheme rs6
```

# 配置 RADIUS 方案的主认证服务器的 IPv6 地址为 2003::2，认证报文的共享密钥设置为明文 123456。

```
[AC1-radius-rs6] primary authentication ipv6 2003::2
```

```
[AC1-radius-rs6] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC1-radius-rs6] user-name-format without-domain
```

```
[AC1-radius-rs6] quit
```

#### (7) 配置 IPv4 认证域

# 创建名为 dm4 的 ISP 域，并进入其视图。

```
[AC1] domain dm4
```

# 配置 Portal 用户使用 RADIUS 方案 rs4 进行认证，不对用户使用的网络服务进行授权和计费。

```
[AC1-isp-dm4] authentication portal radius-scheme rs4
```

```
[AC1-isp-dm4] authorization portal none
```

```
[AC1-isp-dm4] accounting portal none
```

# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小数据流量为 1024 个字节。

```
[AC1-isp-dm4] idle-cut enable 50 1024
```

```
[AC1-isp-dm4] quit
```

#### (8) 配置 IPv6 认证域

# 创建名为 dm6 的 ISP 域，并进入其视图。

```
[AC1] domain dm6
```

# 配置 Portal 用户使用 RADIUS 方案 rs6 进行认证，不对用户使用的网络服务进行授权和计费。

```
[AC1-isp-dm6] authentication portal radius-scheme rs6
```

```

[AC1-isp-dm6] authorization portal none
[AC1-isp-dm6] accounting portal none
# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小
数据流量为 1024 个字节。
[AC1-isp-dm6] idle-cut enable 50 1024
[AC1-isp-dm6] quit
(9) 配置 Portal 支持双机热备
# 配置 VLAN 接口 300 属于 Portal 备份组 1。
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] portal backup-group 1
# 配置接口 VLAN 300 发送 Portal 报文使用的 IPv4 源地址为 192.168.3.100、IPv6 源地址为
3003::100。
[AC1-Vlan-interface300] portal nas-ip 192.168.3.100
[AC1-Vlan-interface300] portal nas-ip ipv6 3003::100
[AC1-Vlan-interface300] quit
# 配置双机热备模式下的设备 ID 为 1，输入“Y”确认。
[AC1] nas device-id 1
Warning: This command will cut all user connections on this device. Continue? [Y/N]Y
# 配置发送 RADIUS 报文使用的源 IPv4 地址为 VRRP 备份组 2 的虚拟 IPv4 地址。
[AC1] radius nas-ip 192.168.100.245
# 配置发送 RADIUS 报文使用的源 IPv6 地址为 VRRP 备份组 2 的虚拟 IPv6 地址。
[AC1] radius nas-ip ipv6 2003::100
# 指定 IPv4 Portal 用户的认证域为 dm4。
[AC1] interface vlan-interface 300
[AC1-Vlan-interface300] portal domain dm4
# 指定 IPv6 Portal 用户的认证域为 dm6。
[AC1-Vlan-interface300] portal domain ipv6 dm6
[AC1-Vlan-interface300] quit
(10) 配置 WLAN 服务
# 配置全局备份 AC 的 IPv4 地址为 192.168.1.2。
[AC1] wlan backup-ac ip 192.168.1.2
# 配置全局备份 AC 的 IPv6 地址为 3001::2。
[AC1] wlan backup-ac ipv6 3001::2
# 使能 AC 间热备份功能。
[AC1] hot-backup enable
# 配置 AC 间用于热备份的 VLAN 为 VLAN 10。
[AC1] hot-backup vlan 10
# 创建接口 WLAN-ESS 1，并设置端口的链路类型为 Hybrid。
[AC1] interface wlan-ess 1
[AC1-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 和 VLAN 300
不带 Tag 通过。
[AC1-WLAN-ESS1] undo port hybrid vlan 1
[AC1-WLAN-ESS1] port hybrid vlan 200 300 untagged

```

```

[AC1-WLAN-ESS1] port hybrid pvid vlan 200
# 使能 MAC VLAN 功能。
[AC1-WLAN-ESS1] mac-vlan enable
[AC1-WLAN-ESS1] quit
# 配置 WLAN 服务模板，SSID 为 service，将接口 WLAN-ESS 1 与该服务模板绑定，并开启 WLAN 服务。
[AC1] wlan service-template 1 clear
[AC1-wlan-st-1] ssid service
[AC1-wlan-st-1] bind wlan-ess 1
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
# 在 AC 1 的 AP 视图下配置 AP 名称为 officeap，型号名称选择 WA2620E-AGN。
[AC1] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC1-wlan-ap-officeap] serial-id 21023529G007C000020
# 配置 AP 的接入优先级设置为 7，该值越大优先级越高，缺省为 4。
[AC1-wlan-ap-officeap] priority level 7
# 进入 radio 2 射频视图。
[AC1-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 300。
[AC1-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC1-wlan-ap-officeap-radio-2] radio enable
[AC1-wlan-ap-officeap-radio-2] quit
[AC1-wlan-ap-officeap] quit
(11) 配置双机热备
# 配置备份 VLAN 为 VLAN 10。
[AC1] dmbk vlan 10
# 使能双机热备功能，且支持对称路径。
[AC1] dmbk enable backup-type symmetric-path

```

### 3.4.2 AC 2 的配置

#### (1) 配置 AC 2 的接口

# 全局使能 IPv6 功能。

```

<AC2> system-view
[AC2] ipv6

```

# 创建 VLAN 10 作为双机热备的 VLAN。

```

[AC2] vlan 10
[AC2-vlan10] quit

```

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv4 和 IPv6 地址。AP 将通过该 VLAN 与 AC 建立 LWAPP 隧道。

```

[AC2] vlan 100
[AC2-vlan100] quit

```

```
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 192.168.1.2 24
[AC2-Vlan-interface100] ipv6 address 3001::2 96
[AC2-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC2] vlan 200
[AC2-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IPv4 和 IPv6 地址。

```
[AC2] vlan 300
[AC2-vlan300] quit
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] ip address 192.168.3.2 24
[AC2-Vlan-interface300] ipv6 address fe80::3 link-local
[AC2-Vlan-interface300] ipv6 address 3003::2 96
[AC2-Vlan-interface300] quit
```

# 创建 VLAN 1 作为与 RADIUS server 通信的 VLAN，并为该接口配置 IPv4 和 IPv6 地址。

```
[AC2] vlan 1
[AC2-vlan1] quit
[AC2] interface vlan-interface 1
[AC2-Vlan-interface1] ip address 192.168.100.163 24
[AC2-Vlan-interface1] ipv6 address fe80::4 link-local
[AC2-Vlan-interface1] ipv6 address 2003::3 64
[AC2-Vlan-interface1] quit
```

# 配置 AC 1 与 AC 2 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access，当前 Access 口允许 VLAN 10 通过。

```
[AC2] interface gigabitethernet 1/0/2
[AC2-GigabitEthernet1/0/2] port link-type access
[AC2-GigabitEthernet1/0/2] port access vlan 10
[AC2-GigabitEthernet1/0/2] quit
```

# 配置 AC 2 下行链路的 GigabitEthernet1/0/3 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，并允许 VLAN 100 和 VLAN 300 的报文通过。

```
[AC2] interface gigabitethernet 1/0/3
[AC2-GigabitEthernet1/0/3] port link-type trunk
[AC2-GigabitEthernet1/0/3] port trunk permit vlan 100 300
[AC2-GigabitEthernet1/0/3] port trunk pvid vlan 100
[AC2-GigabitEthernet1/0/3] quit
```

## (2) 配置 MSTP

# 配置生成树的工作模式为 MSTP。

```
[AC2] stp mode mstp
```

# 激活 MST 域。

```
[AC2] stp region-configuration
[AC2-mst-region] active region-configuration
[AC2-mst-region] quit
```

# 使能 STP 功能。

```
[AC2] stp enable
```

## (3) 配置 VRRP

# 创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IPv4 地址为 192.168.3.100，虚拟 IPv6 地址为 FE80::30 和 3003::100。

```
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] vrrp vrid 1 virtual-ip 192.168.3.100
[AC2-Vlan-interface300] vrrp ipv6 vrid 1 virtual-ip fe80::30 link-local
[AC2-Vlan-interface300] vrrp ipv6 vrid 1 virtual-ip 3003::100
[AC2-Vlan-interface300] quit
```

# 创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IPv4 地址为 192.168.100.245，虚拟 IPv6 地址为 FE80::40 和 2003::100。

```
[AC2] interface vlan-interface 1
[AC2-Vlan-interface1] vrrp vrid 2 virtual-ip 192.168.100.245
[AC2-Vlan-interface1] vrrp ipv6 vrid 2 virtual-ip fe80::40 link-local
[AC2-Vlan-interface1] vrrp ipv6 vrid 2 virtual-ip 2003::100
[AC2-Vlan-interface1] quit
```

#### (4) 配置 Portal 认证

# 配置 IPv4 Portal 服务器：名称为 officev4，IPv4 地址为 192.168.100.240、密钥为明文 123456789，URL 为 http://192.168.100.240:8080/portal。

```
[AC2] portal server officev4 ip 192.168.100.240 key simple 123456789 url
http://192.168.100.240:8080/portal
```

# 配置 IPv6 Portal 服务器：名称为 officev6，IPv6 地址为 2003::2。

```
[AC2] portal server officev6 ipv6 2003::2 key simple 123456789 url
http://[2003::2]:8080/portal
```

# 在 VLAN 接口 300 上配置 Portal 用户报文的控制模式为 MAC，IPv4 或者 IPv6 用户通过 Portal 认证上线后，同时允许该用户的 IPv4 和 IPv6 报文通过认证接口。

```
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] portal control-mode mac
```

# 在 VLAN 接口 300 上使能 Portal 认证，并配置为直接认证方式。

```
[AC2-Vlan-interface300] portal server officev4 method direct
[AC2-Vlan-interface300] portal server officev6 method direct
[AC2-Vlan-interface300] quit
```

#### (5) 配置 IPv4 RADIUS 方案

# 创建名为 rs4 的 RADIUS 方案并进入其视图。

```
[AC2] radius scheme rs4
```

# 配置 RADIUS 方案的主认证服务器的 IPv4 地址为 192.168.100.240，认证报文的共享密钥设置为明文 123456。

```
[AC2-radius-rs4] primary authentication 192.168.100.240
[AC2-radius-rs4] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC2-radius-rs4] user-name-format without-domain
[AC2-radius-rs4] quit
```

#### (6) 配置 IPv6 RADIUS 方案

# 创建名为 rs6 的 RADIUS 方案并进入其视图。

```
[AC2] radius scheme rs6
```

# 配置 RADIUS 方案的主认证服务器的 IPv6 地址为 2003::2，认证报文的共享密钥设置为明文 123456。

```
[AC2-radius-rs6] primary authentication ipv6 2003::2
[AC2-radius-rs6] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC2-radius-rs6] user-name-format without-domain
[AC2-radius-rs6] quit
```

#### (7) 配置 IPv4 认证域

# 创建名为 dm4 的 ISP 域，并进入其视图。

```
[AC2] domain dm4
```

# 配置 Portal 用户使用 RADIUS 方案 rs4 进行认证，不对用户使用的网络服务进行授权和计费。

```
[AC2-isp-dm4] authentication portal radius-scheme rs4
[AC2-isp-dm4] authorization portal none
[AC2-isp-dm4] accounting portal none
```

# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小数据流量为 1024 个字节。

```
[AC2-isp-dm4] idle-cut enable 50 1024
[AC2-isp-dm4] quit
```

#### (8) 配置 IPv6 认证域

# 创建名为 dm6 的 ISP 域，并进入其视图。

```
[AC2] domain dm6
```

# 配置 Portal 用户使用 RADIUS 方案 rs6 进行认证，不对用户使用的网络服务进行授权和计费。

```
[AC2-isp-dm6] authentication portal radius-scheme rs6
[AC2-isp-dm6] authorization portal none
[AC2-isp-dm6] accounting portal none
```

# 允许 ISP 域 office 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小数据流量为 1024 个字节。

```
[AC2-isp-dm6] idle-cut enable 50 1024
[AC2-isp-dm6] quit
```

#### (9) 配置 Portal 支持双机热备

# 配置 VLAN 接口 300 属于 Portal 备份组 1。

```
[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] portal backup-group 1
```

# 配置接口 VLAN 300 发送 Portal 报文使用的 IPv4 源地址为 192.168.3.100、IPv6 源地址为 3003::100。

```
[AC2-Vlan-interface300] portal nas-ip 192.168.3.100
[AC2-Vlan-interface300] portal nas-ip ipv6 3003::100
[AC2-Vlan-interface300] quit
```

# 配置双机热备模式下的设备 ID 为 2，输入“Y”确认。

```
[AC2] nas device-id 2
```

Warning: This command will cut all user connections on this device. Continue? [Y/N]Y

# 配置发送 RADIUS 报文使用的源 IPv4 地址为 VRRP 备份组 2 的虚拟 IPv4 地址。

```
[AC2] radius nas-ip 192.168.100.245
```

# 配置发送 RADIUS 报文使用的源 IPv6 地址为 VRRP 备份组 2 的虚拟 IPv6 地址。

```
[AC1] radius nas-ip ipv6 2003::100
```

# 指定 IPv4 portal 用户的认证域为 dm4。

```

[AC2] interface vlan-interface 300
[AC2-Vlan-interface300] portal domain dm4
# 指定 IPv6 Portal 用户的认证域为 dm6。
[AC2-Vlan-interface300] portal domain ipv6 dm6
[AC2-Vlan-interface300] quit
(10) 配置 WLAN 服务
# 配置全局备份 AC 的 IPv4 地址为 192.168.1.1。
[AC2] wlan backup-ac ip 192.168.1.1
# 配置全局备份 AC 的 IPv6 地址为 3001::1。
[AC1] wlan backup-ac ipv6 3001::1
# 使能 AC 间热备份功能。
[AC2] hot-backup enable
# 配置 AC 间用于热备份的 VLAN 为 VLAN 10。
[AC2] hot-backup vlan 10
# 创建接口 WLAN-ESS 1，并设置端口的链路类型为 Hybrid。
[AC2] interface wlan-ess 1
[AC2-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。
[AC2-WLAN-ESS1] undo port hybrid vlan 1
[AC2-WLAN-ESS1] port hybrid vlan 200 300 untagged
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
[AC2-WLAN-ESS1] mac-vlan enable
[AC2-WLAN-ESS1] quit
# 配置 WLAN 服务模板，SSID 为 service，将接口 WLAN-ESS 1 与该服务模板绑定，并开启 WLAN 服务。
[AC2] wlan service-template 1 clear
[AC2-wlan-st-1] ssid service
[AC2-wlan-st-1] bind wlan-ess 1
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
# 在 AC 2 的 AP 视图下配置 AP 名称为 officeap，型号名称选择 WA2620E-AGN。
[AC2] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC2-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC2-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 300。
[AC2-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC2-wlan-ap-officeap-radio-2] radio enable
[AC2-wlan-ap-officeap-radio-2] quit
[AC2-wlan-ap-officeap] quit
(11) 配置双机热备

```



# 配置备份 VLAN 为 VLAN 10。

```
[AC2] dhrbk vlan 10
```

# 使能双机热备功能，且支持对称路径。

```
[AC2] dhrbk enable backup-type symmetric-path
```

### 3.4.3 Switch 1 的配置

# 全局使能 IPv6 功能。

```
<Switch1> system-view
```

```
[Switch1] ipv6
```

# 配置生成树的工作模式为 MSTP。

```
[Switch1] stp mode mstp
```

# 激活 MST 域。

```
[Switch1] stp region-configuration
```

```
[Switch1-mst-region] active region-configuration
```

```
[Switch1-mst-region] quit
```

# 使能 STP 功能。

```
[Switch1] stp enable
```

### 3.4.4 Switch 2 的配置

(1) 配置 Switch2 的接口

# 全局使能 IPv6 功能。

```
<Switch2> system-view
```

```
[Switch2] ipv6
```

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。

```
[Switch2] vlan 100
```

```
[Switch2-vlan100] quit
```

```
[Switch2] vlan 300
```

```
[Switch2-vlan300] quit
```

# 配置 Switch 2 与 AC 1 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch2] interface gigabitethernet 1/0/1
```

```
[Switch2-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch2-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[Switch2-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch2-GigabitEthernet1/0/1] quit
```

# 配置 Switch 2 与 AC 2 相连的 GigabitEthernet1/0/2 接口链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch2] interface gigabitethernet 1/0/2
```

```
[Switch2-GigabitEthernet1/0/2] port link-type trunk
```

```
[Switch2-GigabitEthernet1/0/2] port trunk permit vlan 100 300
```

```
[Switch2-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

```
[Switch2-GigabitEthernet1/0/2] quit
```

# 配置 Switch 2 与 AP 相连的 GigabitEthernet1/0/3 接口链路类型为 Access，当前 Access 口允许 VLAN 100 通过，并使能 PoE 功能。

```
[Switch2] interface gigabitethernet 1/0/3
[Switch2-GigabitEthernet1/0/3] port link-type access
[Switch2-GigabitEthernet1/0/3] port access vlan 100
[Switch2-GigabitEthernet1/0/3] poe enable
[Switch2-GigabitEthernet1/0/3] quit
```

# 配置生成树的工作模式为 MSTP。

```
[Switch2] stp mode mstp
```

# 激活 MST 域。

```
[Switch2] stp region-configuration
[Switch2-mst-region] active region-configuration
[Switch2-mst-region] quit
```

# 使能 STP 功能。

```
[Switch2] stp enable
```

### 3.4.5 Portal/RADIUS 服务器的配置



说明

下面以 IMC 为例（使用 IMC 版本为：iMC PLAT 7.1(E0303)、iMC EIA 7.1(E0304)、iMC EIP 7.1(E0304)），说明 Portal server、Radius Server 的基本配置。

# 增加接入设备

登录进入 IMC 管理平台，选择“用户”页签，单击导航树中的[接入设备管理/接入设备配置/接入设备配置]菜单项，进入“接入设备配置”页面，在该页面中单击<增加>按钮，进入“增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C(General)”；
- 在设备列表中，单击<手工增加>按钮，添加 IP 地址为 192.168.100.245 的接入设备；
- 单击<增加 IPv6 设备>按钮，进入“手工增加接入设备”页面，填写起始 IP 地址为 2003::100，单击<确定>按钮完成操作；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加 IPv4 接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \*

1812

业务类型

LAN接入业务

接入设备类型

H3C(General)

共享密钥 \*

.....

接入设备分组

无

证书认证

☒不启用 ☐EAP证书认证 ☐WAP证书认证

认证证书类型

EAP-TLS认证

计费端口 \*

1813

业务分组

未分组

确认共享密钥 \*

.....

设备列表

选择手工增加增加IPv6设备全部清除

| 设备名称 | 设备IP地址          | 设备型号 | 备注 | 删除 |
|------|-----------------|------|----|----|
|      | 192.168.100.245 |      |    |    |

图3 增加 IPv6 接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \*

1812

业务类型

LAN接入业务

接入设备类型

H3C(General)

共享密钥 \*

.....

接入设备分组

无

证书认证

☒不启用 ☐EAP证书认证 ☐WAP证书认证

认证证书类型

EAP-TLS认证

计费端口 \*

1813

业务分组

未分组

确认共享密钥 \*

.....

设备列表

选择手工增加增加IPv6设备全部清除

| 设备名称 | 设备IP地址                                  | 设备型号 | 备注 | 删除 |
|------|-----------------------------------------|------|----|----|
|      | 2003:0000:0000:0000:0000:0000:0000:0100 |      |    |    |

- # 增加接入策略。
- 选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入“接入策略管理”页面，单击<增加>按钮，进入“增加接入策略”页面。
- 接入策略名为“portal”，该名称可以自行定义；
  - 业务分组选择“未分组”；
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

帮助

基本信息

接入策略名 \*

portal

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

下发VLAN

☐ 下发User Profile

下发用户组

☐ 下发ACL

# 增加接入服务配置。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入“接入服务管理”页面，在该页面中单击<增加>按钮，进入“增加接入服务”页面。

- 输入服务名“portal auth”，该名称可以自行定义；
- 业务分组“未分组”；
- 缺省接入策略“portal”，即上一步配置的接入策略名；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

帮助

基本信息

服务名 \*

portal auth

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

portal

缺省私有属性下发策略 \*

不使用

缺省单帐号最大绑定终端数 \*

0

缺省单帐号在线数量限制 \*

0

服务描述

☒ 可申请

☒ 无感知认证

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“admin”；
- 输入证件号码“12345”；
- 单击<检查是否可用>按钮；

- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图6 增加用户

增加用户

基本信息

用户姓名 \*

admin

✓

证件号码 \*

12345

✓

检查是否可用

通讯地址

电话

?

电子邮件

?

用户分组 \*

未分组

确定

取消

在“增加接入用户”页面，按如下方式配置。

- 输入账号名“portal”；
- 输入密码“123456”；
- 接入服务选择“portal auth”；
- 其他配置保持默认；
- 单击<确定>按钮完成操作。

图7 增加接入用户

接入信息

用户姓名 \*

admin

选择

增加用户

帐号名 \*

portal

☐ 预开户用户

☐ 缺省BYOD用户

☐ MAC地址认证用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

时

失效时间

时

最大闲置时长(分钟)

在线数量限制

1

登录提示信息

接入服务

| 服务名                                             | 服务后缀 | 状态  | 分配IP地址 |
|-------------------------------------------------|------|-----|--------|
| <input type="checkbox"/> dot1x-w                |      | 可申请 |        |
| <input checked="" type="checkbox"/> portal auth |      | 可申请 |        |

# 配置 Portal 主页

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入“服务器配置”页面，配置 Portal 主页，采用默认配置即可，单击<确定>按钮完成。

图8 服务器配置

用户 > 接入策略管理 > Portal服务器配置

告警浏览  
告警设置  
安全控制中心  
Trap管理  
Syslog管理

Portal服务器配置

基本信息

日志级别 \* 信息

Portal Server

报文请求超时长(秒) \* 4 逃生心跳间隔时长(秒) \* 20

用户心跳间隔时长(分钟) \* 5 LB设备地址

LB设备IPv6地址

Portal Web

请求报文超时长(秒) \* 15 交互报文编码

校验终端用户请求报文 是 使用缓存 是

HTTP心跳界面展示方式 新页面 HTTPS心跳界面展示方式 原页面

Portal主页

http://192.168.100.240:8080/portal/  
https://192.168.100.240:8443/portal/  
http://[2003::2]:8080/portal/  
https://[2003::2]:8443/portal/

# 配置 Portal 认证的地址组范围

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，单击<增加>按钮，配置 Portal 认证的地址组范围。

- 填写 IP 地址组名；
- IPv6 选择“是”（仅 IPv6，IPv4 地址选“否”）；
- 输入起始地址和终止地址，输入的地址范围中应包含用户主机的 IP 地址；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。（仅 IPv4 地址组配置本项）

图9 增加 IPv4 地址组

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组

增加IP地址组

IP地址组名 \* portal4

IPv6 \* 否

起始地址 \* 192.168.3.1

终止地址 \* 192.168.3.255

业务分组 未分组

类型 \* 普通

确定 取消

图10 增加 IPv6 地址组配置页面

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组

帮助

增加IPv6地址组

IP地址组名 \*

portal6

IPv6 \*

是

起始地址 \*

3003::1

终止地址 \*

3003::FFFF:FFFF

业务分组

未分组

确定

取消

# 配置接入设备信息

选择“用户”页签，单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，单击“增加”按钮，配置 Portal 认证的接入设备。

- 填写设备名；
- IPv4 用户版本选择“Portal 2.0”，IPv6 用户版本选择“Portal 3.0”；
- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 选择是否支持逃生心跳功能和用户心跳功能，本例中选择否。
- 输入密钥，与 AC 上的配置保持一致；
- 选择组网方式为直连；
- 其它参数可采用缺省配置。

图11 增加 IPv4 设备信息

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

帮助

增加设备信息

设备信息

设备名 \*

AC4

业务分组 \*

未分组

版本 \*

Portal 2.0

IP地址 \*

192.168.3.100

监听端口 \*

2000

本地Challenge \*

否

认证重发次数 \*

0

下线重发次数 \*

1

支持逃生心跳 \*

否

支持用户心跳 \*

否

密钥 \*

.....

确认密钥 \*

.....

组网方式 \*

直连

设备描述

确定

取消

图12 增加 IPv6 设备信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

增加设备信息

设备信息

设备名 \*

AC6

版本 \*

Portal 3.0

监听端口 \*

2000

认证重发次数 \*

0

支持逃生心跳 \*

否

密钥 \*

.....

组网方式 \*

直连

设备描述

业务分组 \*

未分组

IP地址 \*

3003::100

本地Challenge \*

否

下线重发次数 \*

1

支持用户心跳 \*

否

确认密钥 \*

.....

确定

取消

# 配置端口组

返回[用户接入管理/Portal 服务管理/设备配置]菜单项，在“设备信息列表”中点击 AC4 或者 AC6 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图13 设备配置

用户 > 接入策略管理 > Portal服务管理 > 设备配置

★ 加入收藏 ? 帮助

设备信息查询

设备名

版本

下发结果

业务分组

查询

重置

增加

| 设备名 | 版本         | 业务分组 | IP地址          | IPv6地址    | 最近一次下发时间 | 下发结果 | 操作                                                      |
|-----|------------|------|---------------|-----------|----------|------|---------------------------------------------------------|
| AC6 | Portal 3.0 | 未分组  |               | 3003::100 |          | 未下发  | <div><div></div><div></div><div></div><div></div></div> |
| AC4 | Portal 2.0 | 未分组  | 192.168.3.100 |           |          | 未下发  | <div><div></div><div></div><div></div><div></div></div> |

共有2条记录，当前第1 - 2，第 1/1 页。

<<

<

1

>

>>

50

在“端口组信息列表”子页签，单击<增加>按钮，进入到“增加端口组信息”页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其他采用默认配置即可；
- 单击<确定>按钮完成操作。



图14 增加 IPv4 端口组信息

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 增加端口组信息

增加端口组信息

端口组名 \*

G4

开始端口 \*

0

协议类型 \*

HTTP

是否NAT \*

否

认证方式 \*

CHAP认证

心跳间隔(分钟) \*

0

用户域名

无感知认证

不支持

页面推送策略

提示语言 \*

动态检测

终止端口 \*

zzzzzz

快速认证 \*

否

错误透传 \*

是

IP地址组 \*

portal4

心跳超时(分钟) \*

0

端口组描述

客户端防破解 \*

否

缺省认证页面

确定

取消

图15 增加 IPv6 端口组信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 增加端口组信息

增加端口组信息

端口组名 \*

G6

开始端口 \*

0

协议类型 \*

HTTP

是否NAT \*

否

认证方式 \*

CHAP认证

心跳间隔(分钟) \*

0

用户域名

无感知认证

不支持

页面推送策略

提示语言 \*

动态检测

终止端口 \*

zzzzzz

快速认证 \*

否

错误透传 \*

是

IP地址组 \*

portal6

心跳超时(分钟) \*

0

端口组描述

客户端防破解 \*

否

缺省认证页面

确定

取消

3.5 验证配置

# Client 从 AC 1 成功上线后,在 AC 1 上通过命令 **display portal user all** 查看该用户的认证情况。可以看到 Portal 用户的工作模式为主用户模式 **primary**，表示该用户是由 AC 1 上线。

```
[AC1] display portal user all
Index:0
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:primary
MAC          IP          Vlan    Interface
```

```
-----
3ca9-f414-4c20 192.168.3.5 300 Vlan-interface300
```

```
Total 1 user(s) matched, 1 listed.
```

# Client 从 AC 1 成功上线后，在 AC 2 通过命令 **display portal user all** 查看该用户的认证情况。可以看到 Portal 用户的工作模式为备用户模式 **secondary**，表示该用户的认证信息同步到 AC 2 上。

```
[AC2] display portal user all
```

```
Index:0
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode:secondary
```

```
MAC IP Vlan Interface
```

```
-----
3ca9-f414-4c20 192.168.3.5 300 Vlan-interface300
```

```
Total 1 user(s) matched, 1 listed.
```

# 通过将 AC 1 下电模拟主 AC 宕机的情形，使得 AC 发生主备切换，此时，在 AC 2 上便可以查看到用户的状态由“secondary”转换为“stand-alone”状态，说明此时只有 AC 2 处于工作状态。

```
[AC2] display portal user all
```

```
Index:0
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode:stand-alone
```

```
MAC IP Vlan Interface
```

```
-----
3ca9-f414-4c20 192.168.3.5 300 Vlan-interface300
```

```
Total 1 user(s) matched, 1 listed.
```

## 3.6 配置文件

- AC 1 的配置文件：

```
#
radius nas-ip ipv6 2003::0100
nas device-id 1
#
ipv6
#
portal server officev4 ip 192.168.100.240 key cipher $c$3$k404VUVwII8mp/Re6WpNU
wk4JrBbXsRiUzYb9A== url http://192.168.100.240:8080/portal server-type imc
portal server officev6 ipv6 2003::2 key cipher $c$3$bP0W+eBZJdxE/mKXlGmoGilc/gW
kv0y6abC6PQ== url http://[2003::2]:8080/portal server-type imc
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
#
wlan backup-ac ip 192.168.1.2
wlan backup-ac ipv6 3001::2
#
hot-backup enable domain 1
```

```

hot-backup vlan 10
#
vlan 1
#
vlan 10
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme rs6
  primary authentication ipv6 2003::0002
  primary accounting ipv6 2003::0002
  key authentication cipher $c$3$YvYFuVf9PIY6Jg/eYeuH7VLV0vbhAmh0gg==
  user-name-format without-domain
radius scheme rs4
  primary authentication 192.168.100.240
  primary accounting 192.168.100.240
  key authentication cipher $c$3$zdQLHG1FGgNpAuye0JS3331P6s0KQNvmrw==
  key accounting cipher $c$3$OIc+iiVqnz13BQBHa/LiDTlVVIFQ0RbZJA==
  user-name-format without-domain
#
domain dm4
  authentication portal radius-scheme rs4
  authorization portal none
  accounting portal none
  access-limit disable
  state active
  idle-cut enable 50 1024
  self-service-url disable
domain dm6
  authentication portal radius-scheme rs6
  authorization portal none
  accounting portal none
  access-limit disable
  state active
  idle-cut enable 50 1024
  self-service-url disable
#
stp instance 0 root primary
stp enable
#
wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable

```

```

#
interface Vlan-interface1
  ipv6 address 2003::1/64
  ipv6 address FE80::2 link-local
  ip address 192.168.100.147 255.255.255.0
  vrrp vrid 2 virtual-ip 192.168.100.245
  vrrp vrid 2 priority 254
  vrrp ipv6 vrid 2 virtual-ip FE80::40 link-local
  vrrp ipv6 vrid 2 virtual-ip 2003::100
  vrrp ipv6 vrid 2 priority 254
#
interface Vlan-interface10
  ipv6 address 3010::1/96
  ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface100
  ipv6 address 3001::1/96
  ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface200
#
interface Vlan-interface300
  ipv6 address 3003::1/96
  ipv6 address FE80::1 link-local
  ip address 192.168.3.1 255.255.255.0
  vrrp vrid 1 virtual-ip 192.168.3.100
  vrrp vrid 1 priority 254
  vrrp ipv6 vrid 1 virtual-ip FE80::30 link-local
  vrrp ipv6 vrid 1 virtual-ip 3003::100
  vrrp ipv6 vrid 1 priority 254
  portal control-mode mac
  portal server officev4 method direct
  portal server officev6 method direct
  portal domain dm4
  portal domain ipv6 dm6
  portal backup-group 1
  portal nas-ip 192.168.3.100
  portal nas-ip ipv6 3003::100
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 300
#
interface GigabitEthernet1/0/2
  port link-type trunk
  port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/3

```

```

port access vlan 10
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 300 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio enable
radio 2
service-template 1 vlan-id 300
radio enable
#
dhrb enable backup-type symmetric-path
dhrb vlan 10
#
return
#

```

- AC 2 的配置文件:

```

#
radius nas-ip ipv6 2003::0100
nas device-id 2
#
ipv6
#
portal server officev4 ip 192.168.100.240 key cipher $c$3$mxac233QhDqkyRJvd9EeX
NOMM8DKhZyITJctNA== url http://192.168.100.240:8080/portal server-type imc
portal server officev6 ipv6 2003::2 key cipher $c$3$G0WJL9a+wgLa8WMMBncBj83nPk9
S7nTYmMlpOg== url http://[2003::2]:8080/portal server-type imc
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
#
wlan backup-ac ip 192.168.1.1
wlan backup-ac ipv6 3001::1
#
hot-backup enable domain 1
hot-backup vlan 10
#
vlan 1
#
vlan 10
#
vlan 100
#
vlan 200

```

```

#
vlan 300
#
radius scheme rs4
    primary authentication 192.168.100.240
    key authentication cipher $c$3$ezwUorHFXLxU0eaO2OyoyURVFuZwUNflAA==
    user-name-format without-domain
radius scheme rs6
    primary authentication ipv6 2003::0002
    key authentication cipher $c$3$+qsA4GoP0aSDprsQyjFcsijBFDr2wsISTg==
    user-name-format without-domain
#
domain dm4
    authentication portal radius-scheme rs4
    authorization portal none
    accounting portal none
    access-limit disable
    state active
    idle-cut enable 50 1024
    self-service-url disable
domain dm6
    authentication portal radius-scheme rs6
    authorization portal none
    accounting portal none
    access-limit disable
    state active
    idle-cut enable 50 1024
    self-service-url disable
#
    stp enable
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
interface NULL0
#
interface Vlan-interface1
    ipv6 address 2003::3/64
    ipv6 address FE80::4 link-local
    ip address 192.168.100.163 255.255.255.0
    vrrp vrid 2 virtual-ip 192.168.100.245
    vrrp ipv6 vrid 2 virtual-ip FE80::40 link-local
    vrrp ipv6 vrid 2 virtual-ip 2003::100
#
interface Vlan-interface10
    ipv6 address 3010::2/96

```

```

ip address 192.168.10.2 255.255.255.0
#
interface Vlan-interface100
  ipv6 address 3001::2/96
  ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface200
#
interface Vlan-interface300
  ipv6 address 3003::2/96
  ipv6 address FE80::3 link-local
  ip address 192.168.3.2 255.255.255.0
  vrrp vrid 1 virtual-ip 192.168.3.100
  vrrp ipv6 vrid 1 virtual-ip FE80::30 link-local
  vrrp ipv6 vrid 1 virtual-ip 3003::100
  portal control-mode mac
  portal server officev4 method direct
  portal server officev6 method direct
  portal domain dm4
  portal domain ipv6 dm6
  portal backup-group 1
  portal nas-ip 192.168.3.100
  portal nas-ip ipv6 3003::100
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 300
#
interface GigabitEthernet1/0/2
  port link-type trunk
  port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/3
  port access vlan 10
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 300 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
  service-template 1 vlan-id 300
  radio enable

```

```
#
dhrb enable backup-type symmetric-path
dhrb vlan 10
#
return
```

- Switch 1 的配置文件:

```
#
stp enable
#
```

- L2 Switch 的配置文件:

```
#
dhcp enable
#
ipv6 dhcp server forbidden-address 3001::1 3001::4
ipv6 dhcp server forbidden-address 3003::1 3003::4
#
#
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#
stp global enable
#
dhcp server ip-pool 100
network 192.168.1.0 mask 255.255.255.0
#
dhcp server ip-pool 300
network 192.168.3.0 mask 255.255.255.0
#
ipv6 dhcp pool 1
network 3001::/96
#
ipv6 dhcp pool 2
network 3003::/96
#
ipv6 dhcp pool global
#
interface NULL0
#
interface Vlan-interface100
ip address 192.168.1.3 255.255.255.0
ipv6 dhcp select server
ipv6 dhcp server apply pool 1
```



```

ipv6 address 3001::3/96
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface Vlan-interface300
ip address 192.168.3.3 255.255.255.0
ipv6 dhcp select server
ipv6 dhcp server apply pool 2
ipv6 address 3003::3/96
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 300
#
interface GigabitEthernet1/0/2
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 1 100 300
poe enable
#
return

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“可靠性配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“可靠性命令参考”。

# IPv6 本地 Portal 认证基于 SSID 绑定认证页面 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                               |    |
|-------------------------------|----|
| 1 简介.....                     | 1  |
| 2 配置前提 .....                  | 1  |
| 3 配置举例 .....                  | 1  |
| 3.1 组网需求 .....                | 1  |
| 3.2 配置思路 .....                | 1  |
| 3.3 配置注意事项 .....              | 2  |
| 3.4 配置步骤 .....                | 2  |
| 3.4.1 AC 的配置 .....            | 2  |
| 3.4.2 Switch 的配置 .....        | 5  |
| 3.4.3 RADIUS server 的配置 ..... | 5  |
| 3.5 验证配置 .....                | 8  |
| 3.6 配置文件 .....                | 9  |
| 4 相关资料 .....                  | 11 |

# 1 简介

本文档介绍本地 Portal 认证基于 SSID 绑定认证页面的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、WLAN 无线接入、Portal 认证特性。

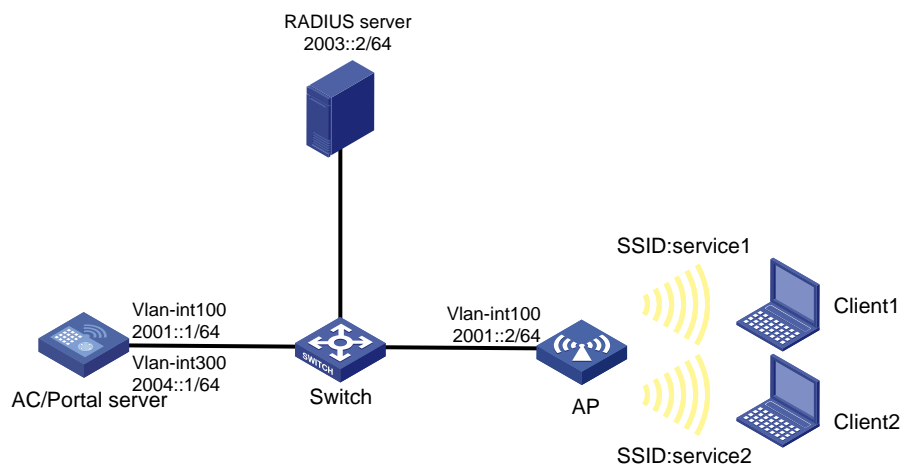
## 3 配置举例

### 3.1 组网需求

如图 1 所示，RADIUS 服务器作为认证/计费服务器，Switch 作为 DHCPv6 服务器为 AP 和 Client 分配 IPv6 地址。要求通过基于 SSID 绑定本地 Portal 认证页面的功能，实现：

- 当无线客户端通过名为 service1 的 SSID 接入网络时，Portal 认证推出自定义的认证页面；
- 当无线客户端通过名为 service2 的 SSID 接入网络时，Portal 认证推出的是系统默认认证页面。

图1 本地 Portal 认证基于 SSID 绑定认证页面组网图



### 3.2 配置思路

为了使无线客户端从 service1 接入时推出自定义认证页面，需编辑自定义认证页面并上传至 AC。

### 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.4 配置步骤

#### 3.4.1 AC 的配置

##### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。AC 将使用该接口的 IPv6 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 address 2001::1 64
# 取消对 RA 消息发布的抑制。
[AC-Vlan-interface100] undo ipv6 nd ra halt
# 设置被管理地址配置标志位为 1。
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
# 设置其他配置标志位为 1。
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并配置其接口 IPv6 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ipv6 address 2004::1 64
# 取消对 RA 消息发布的抑制。
[AC-Vlan-interface300] undo ipv6 nd ra halt
# 设置被管理地址配置标志位为 1。
[AC-Vlan-interface300] ipv6 nd autoconfig managed-address-flag
# 设置其他配置标志位为 1。
[AC-Vlan-interface300] ipv6 nd autoconfig other-flag
[AC-Vlan-interface300] quit
```

# 配置 AC 连接 Switch 的 GigabitEthernet1/0/1 接口的属性为 trunk，并允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置认证策略和认证域

# 在 AC 上创建 RADIUS 方案 office 并进入其视图。

```
[AC] radius scheme office
```

# 配置 RADIUS 方案的主认证服务器及其通信密钥。

```
[AC-radius-office] primary authentication ipv6 2003::2
```

```
[AC-radius-office] key authentication 123456
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC-radius-office] user-name-format without-domain
```

```
[AC-radius-office] quit
```

# 配置发送 RADIUS 报文的源 IPv6 地址为 2001::1。

```
[AC] radius nas-ip ipv6 2001::1
```

# 创建并进入名字为 office 的 ISP 域视图。

```
[AC] domain office
```

# 为 Portal 用户配置 AAA 认证方法为 RADIUS 认证/授权方案 office，不计费。

```
[AC-isp-office] authentication portal radius-scheme office
```

```
[AC-isp-office] authorization portal radius-scheme office
```

```
[AC-isp-office] accounting portal none
```

```
[AC-isp-office] quit
```

## (3) 配置 Portal

# 配置 Portal 服务器：名称为 office，IPv6 地址为 2001::1。

```
[AC] portal server office ipv6 2001::1
```

# 配置本地 Portal 服务器支持 HTTP 协议。

```
[AC] portal local-server http
```

# 在用户所在的 VLAN 300 接口上使能 Portal。

```
[AC] interface vlan-interface 300
```

```
[AC-Vlan-interface300] portal server office method direct
```

# 指定 Portal 用户的认证域为 office。

```
[AC-Vlan-interface300] portal domain ipv6 office
```

```
[AC-Vlan-interface300] quit
```

## (4) 配置 WLAN 服务

# 创建接口 WLAN-ESS 1，并设置端口的链路类型为 Hybrid。

```
[AC] interface wlan-ess 1
```

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

# 创建接口 WLAN-ESS 2，并设置端口的链路类型为 Hybrid。

```
[AC] interface wlan-ess 2
```

```
[AC-WLAN-ESS2] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS2] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS2] port hybrid vlan 200 untagged
[AC-WLAN-ESS2] port hybrid pvid vlan 200
[AC-WLAN-ESS2] mac-vlan enable
[AC-WLAN-ESS2] quit
```

# 配置 WLAN 服务模板 1，SSID 为 **service1**，并将接口 WLAN-ESS 1 与该服务模板绑定，启用无线服务。

```
[AC] wlan service-template 1 clear
[AC-wlan-st-1] ssid service1
[AC-wlan-st-1] bind wlan-ess 1
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

# 配置 WLAN 服务模板 2，SSID 为 **service2**，并将接口 WLAN-ESS 2 与该服务模板绑定，启用无线服务。

```
[AC] wlan service-template 2 clear
[AC-wlan-st-2] ssid service2
[AC-wlan-st-2] bind wlan-ess 2
[AC-wlan-st-2] service-template enable
[AC-wlan-st-2] quit
```

# 创建 AP 的管理模板，名称为 **officeap**，型号名称选择 **WA2620E-AGN**，并配置 AP 的序列号。

```
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 **radio 2** 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将服务模板 1 和 2 绑定到 AP 的 **Radio 2** 口，配置绑定到 **Radio 2** 口的 **VLAN** 为 **VLAN 300**，并使能 **Radio 2**。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
[AC-wlan-ap-officeap-radio-2] service-template 2 vlan-id 300
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

## (5) 将自定义认证页面文件上传至 AC

# 通过 **FTP** 将本地的自定义认证页面文件 **ssid1.zip** 上传至 **AC**（过程略），并用 **dir \*.zip** 命令查看上传完的文件。

```
<AC> dir *.zip
Directory of cfa0:/
0      -rw-      66127  Nov 27 2013 10:39:08  ssid1.zip
1020068 KB total (502420 KB free)
File system type of cfa0: FAT32
```

## (6) 配置 SSID 绑定自定义页面文件

# 将 **SSID: service 1** 与页面文件 **ssid1.zip** 绑定。

```
<AC> system-view
[AC] portal local-server bind ssid service1 file ssid1.zip
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 trunk, 当前 trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 access, 并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 使能 DHCPv6 服务器功能。

```
[Switch] ipv6 dhcp server enable
```

# 创建 DHCPv6 地址池 1, 配置地址池范围为 2001::/64, 为 AP 分配 IPv6 地址。

```
[Switch] ipv6 dhcp pool 1
[Switch-dhcp6-pool-1] network 2001::/64
[Switch-dhcp6-pool-1] quit
```

# 创建 DHCPv6 地址池 2, 配置地址池范围为 2004::/64, 为 Client 分配 IPv6 地址。

```
[Switch] ipv6 dhcp pool 2
[Switch-dhcp6-pool-2] network 2004::/64
[Switch-dhcp6-pool-2] quit
```

### 3.4.3 RADIUS server 的配置



说明

下面以 iMC 为例(使用 iMC 版本为: iMC PLAT 7.0 (E0202)、iMC UAM 7.0 (E0202), 说明 RADIUS server 的基本配置。

---

# 增加接入设备

登录进入 iMC 管理平台, 选择“用户”页签, 单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项, 单击“增加”按钮, 进入“增加接入设备”页面, 单击<增加 IPv6 设备>按钮, 进入“手工增加接入设备”页面。



- 填写起始 IPv6 地址为 2001::1，该 IPv6 地址为 AC 上配置的 radius scheme 视图下的 nas-ip 地址。
- 单击<确定>按钮完成操作。
- 在“接入配置”页面配置共享密钥为 123456，该共享密钥与 AC 上配置 RADIUS 服务器时的密钥一致。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

## # 配置接入策略

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，点击<增加>按钮，进入“增加接入策略”页面。

- 接入策略名填写 portal。该名称可以自行定义。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

## # 配置接入服务

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，点击<增加>按钮，进入“增加接入服务”页面。

- 服务名填写 portal。该名称可以自行定义。
- 缺省接入策略选择“portal”。即上一步配置的接入策略名。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

基本信息

服务名 \*

portal

业务分组 \*

未分组

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 (PC)

服务描述

☒可申请

☐Portal无感知认证

服务后缀

缺省接入策略 \*

portal

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

## # 配置接入用户

选择“用户”页签，单击导航树中的[增加用户]菜单项，进入“增加用户”页面。

- 用户姓名填写 **Test**。该名称可以自行定义。
- 证件号码填写 **123**。该名称可以自行定义。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 增加用户 帮助

增加用户

基本信息

用户姓名 \*

Test

证件号码 \*

123

通讯地址

电子邮件

电话

用户分组 \*

未分组

☐开通自助帐户

确定

取消

添加用户完成后，会跳转到“增加用户结果页面”，单击[增加用户账号]进入“增加接入用户”视图。

用户 > 增加用户结果 帮助

增加用户完成，您可继续选择如下操作：

[增加用户账号](#)

[返回用户列表](#)

[查看用户详细信息](#)

[继续增加用户](#)

增加接入用户帐号。

返回用户列表。

查看刚刚增加的用户的信息。

继续增加新的用户。

在“增加接入用户”视图下。

- 账户名填写 **test**。该名称可以自行定义。
- 密码填写 **123456**。该名称可以自行定义。
- 接入服务选择上一步配置的接入服务“portal”。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 接入用户 > 增加接入用户

接入用户

接入信息

用户姓名 \*  选择 增加用户

帐号名 \*

☐ 桥开户用户 ☐ 缺省BYOD用户 ☐ 主机名用户 ☐ 快速认证用户

密码 \*  密码确认 \*

☒ 允许用户修改密码 ☐ 启用用户密码控制策略 ☐ 下次登录须修改密码

生效时间  失效时间

最大闲置时长(分钟)  在线数量限制

Portal无感知认证最大绑定数

登录提示信息

接入服务

| 服务名                               | 服务后缀 | 状态  | 分配IP地址 |
|-----------------------------------|------|-----|--------|
| <input type="checkbox"/> lyportal |      | 可申请 |        |
| <input type="checkbox"/> mp       |      | 可申请 |        |
| ... portal                        |      | 可申请 |        |

## 3.5 验证配置

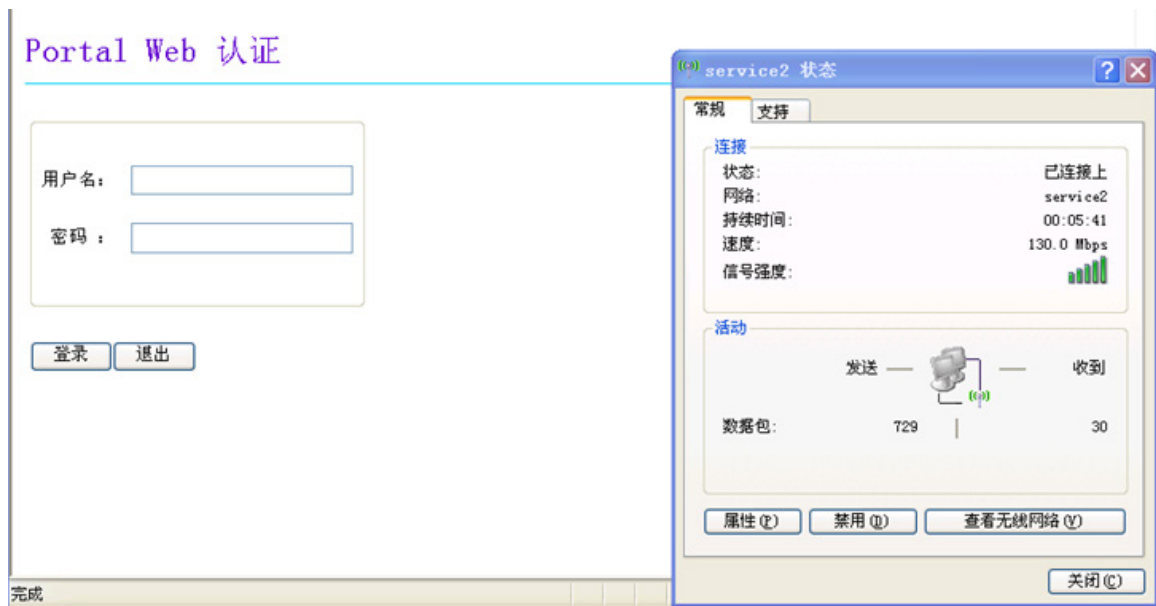
# Client 1 通过无线服务 service 1 上线后，进行 Portal 认证时，弹出自定义的认证页面。

图2 自定义认证页面



# Client 2 通过无线服务 service 2 上线后，由于没有配置其绑定的自定义认证页面，所以客户端进行 Portal 认证时推出的是系统默认认证页面。

图3 系统默认认证页面



## 3.6 配置文件

- AC:

```
#
radius nas-ip ipv6 2001::0001
#
portal server office ipv6 2001::1 server-type imc
portal local-server http
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
primary authentication ipv6 2003::0002
key authentication cipher $c$3$lRA4cjtdvxqsRUuMR42kkQWa3b9Yw9Hk7A==
user-name-format without-domain
#
domain office
authentication portal radius-scheme office
authorization portal radius-scheme office
accounting portal none
access-limit disable
state active
idle-cut disable
self-service-url disable
```

```

#
wlan service-template 1 clear
  ssid service1
  bind WLAN-ESS 1
  service-template enable
#
wlan service-template 2 clear
  ssid service2
  bind WLAN-ESS 2
  service-template enable
#
interface Vlan-interface100
  undo ipv6 nd ra halt
  ipv6 nd autoconfig managed-address-flag
  ipv6 nd autoconfig other-flag
  ipv6 address 2001::1/64
  ipv6 dhcp server apply pool 1

#
interface Vlan-interface300
  undo ipv6 nd ra halt
  ipv6 nd autoconfig managed-address-flag
  ipv6 nd autoconfig other-flag
  ipv6 address 2001::1/64
  ipv6 dhcp server apply pool 1
  portal server office method direct
  portal domain ipv6 office
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200 300
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
interface WLAN-ESS2
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020

```

```

radio 1
radio 2
  service-template 1 vlan-id 300
  service-template 2 vlan-id 300
radio enable
#
•   Switch:
#
ipv6 dhcp server enable
#
vlan 100
#
vlan 300
#
ipv6 dhcp pool 1
  network 2001::/64
#
ipv6 dhcp pool 2
  network 2004::/64
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 100 300
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
  poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“三层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“三层技术命令参考”。

# 本地 Portal server 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                           |    |
|---------------------------|----|
| 1 简介.....                 | 1  |
| 2 配置前提 .....              | 1  |
| 3 配置举例 .....              | 1  |
| 3.1 组网需求 .....            | 1  |
| 3.2 配置思路 .....            | 2  |
| 3.3 配置注意事项 .....          | 2  |
| 3.4 配置步骤 .....            | 2  |
| 3.4.1 AC 的配置 .....        | 2  |
| 3.4.2 Switch 的配置 .....    | 5  |
| 3.4.3 RADIUS 服务器的配置 ..... | 5  |
| 3.5 验证配置 .....            | 9  |
| 3.6 配置文件 .....            | 10 |
| 4 相关资料 .....              | 12 |



# 1 简介

本文介绍了在 WLAN 接入中使用本地 Portal 认证特性的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 Portal 认证的特性。

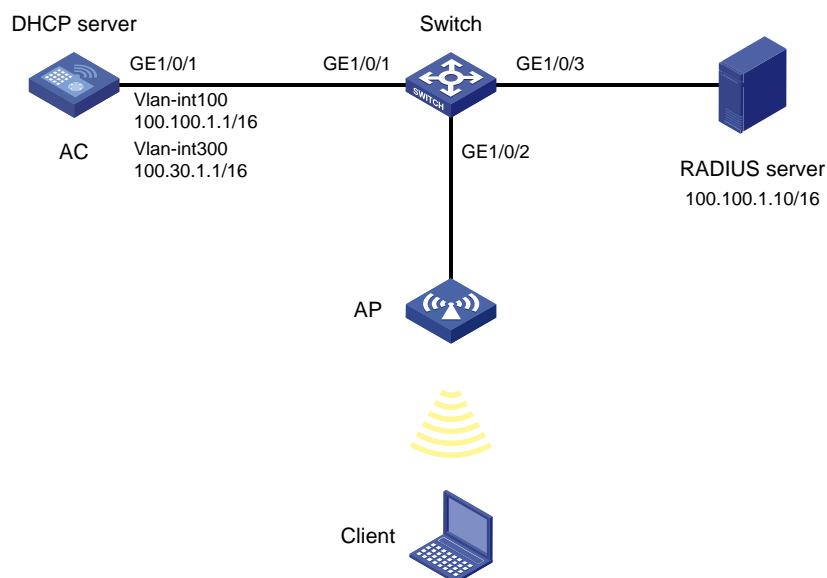
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，Client 通过无线网络访问内部局域网，AC 通过 Switch 连接 AP 和 RADIUS 服务器，Switch 作为 DHCP 服务器，为 Client 和 AP 提供 IP 地址。现要求：

- 要求 AC 使用本地 Portal 认证的方式对接入的 Client 进行认证，只有通过认证的 Client 才能够访问局域网
- 使用 RADIUS 服务器进行认证、授权和计费。

图1 本地 Portal Server 组网图



## 3.2 配置思路

- 为实现 AP 和 Client 可以自动获取 IP 地址的功能，在 AC 上开启 DHCP 服务器功能。
- 为了实现对 Client 进行 Portal 认证，需要配置 RADIUS 方案和认证域。

## 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 100.100.1.1 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 100.30.1.1 255.255.0.0
[AC-Vlan-interface300] quit
```

# 配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 DHCP 服务

# 创建名为 vlan100 的 DHCP 地址池，动态分配的网段为 100.100.1.0/16，网关地址为 100.100.1.1。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 100.100.1.0 mask 255.255.0.0
[AC-dhcp-pool-vlan100] gateway-list 100.100.1.1
```

```

[AC-dhcp-pool-vlan100] quit
# 创建名为 vlan300 的 DHCP 地址池，动态分配的网段为 100.30.1.0/16，网关地址为 100.30.1.1。
[AC] dhcp server ip-pool vlan300
[AC-dhcp-pool-vlan300] network 100.30.1.0 mask 255.255.0.0
[AC-dhcp-pool-vlan300] gateway-list 100.30.1.1
[AC-dhcp-pool-vlan300] quit
# 使能 DHCP 服务。
[AC] dhcp enable

```

### (3) 配置认证策略

```

# 创建 RADIUS 方案 office 并进入其视图。
[AC] radius scheme office
# 将 RADIUS 方案 office 的 RADIUS 服务器类型设置为 extended。
[AC-radius-office] server-type extended
# 设置主认证 RADIUS 服务器的 IP 地址 100.100.1.10。
[AC-radius-office] primary authentication 100.100.1.10
# 设置主计费 RADIUS 服务器的 IP 地址 100.100.1.10。
[AC-radius-office] primary accounting 100.100.1.10
# 设置系统与认证 RADIUS 服务器交互报文时的共享密钥为 admin。
[AC-radius-office] key authentication admin
# 设置系统与计费 RADIUS 服务器交互报文时的共享密钥为 admin。
[AC-radius-office] key accounting admin
# 配置发送给 RADIUS 方案 office 中 RADIUS 服务器的用户名不携带 ISP 域名。
[AC-radius-office] user-name-format without-domain
[AC-radius-office] quit

```

### (4) 配置认证域

```

# 创建 office 域并进入其视图。
[AC] domain office
# 为 Portal 用户配置认证方案为 RADIUS 方案，方案名为 office。
[AC-isp-office] authentication portal radius-scheme office
# 为 Portal 用户配置授权方案为 RADIUS 方案，方案名为 office。
[AC-isp-office] authorization portal radius-scheme office
# 为 Portal 用户配置计费方案为 RADIUS 方案，方案名为 office。
[AC-isp-office] accounting portal radius-scheme office
[AC-isp-office] quit
# 把配置的认证域 office 设置为系统缺省的 ISP 域。
[AC] domain default enable office

```

### (5) 配置 WLAN-ESS 接口

```

# 创建 WLAN-ESS 1 接口，并进入该视图。
[AC] interface wlan-ess 1
# 配置端口的链路类型为 Hybrid。
[AC-WLAN-ESS1] port link-type hybrid
# 配置接口 WLAN-ESS1 的缺省 VLAN 为 VLAN 200，禁止 VLAN 1 报文通过，并允许发送 VLAN 200 报文不带 VLAN tag。

```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

#### (6) 配置无线服务模板

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置服务模板 1 的 SSID（服务模板的标识）为 office。

```
[AC-wlan-st-1] ssid office
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 使能服务模板。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

#### (7) 在 AC 下绑定无线服务模板

# 创建 AP 管理模板，其名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-officeap] radio 1
```

# 将在 AC 上配置的服务模板 1 映射到射频 1，设置绑定到射频接口的 VLAN 编号为 VLAN 300。

```
[AC-wlan-ap-officeap-radio-1] service-template 1 vlan 300
```

# 使能 AP 的 radio 1。

```
[AC-wlan-ap-officeap-radio-1] radio enable
[AC-wlan-ap-officeap-radio-1] quit
[AC-wlan-ap-officeap] quit
```

#### (8) 配置 Portal Server 和免认证规则

# 配置 Portal 服务器的 IP 地址为 100.30.1.1，并为该 Portal 服务器命名为 office。

```
[AC] portal server office ip 100.30.1.1
```

# 配置 Portal 免认证规则 0，符合源接口为 GigabitEthernet 1/0/1 的任意报文不会触发 Portal 认证。

```
[AC] portal free-rule 0 source interface GigabitEthernet 1/0/1 destination any
```

# 配置本地 Portal 服务器支持 HTTP 协议方式。

```
[AC] portal local-server http
```

# 在接口 VLAN 300 上使能 Portal，指定 Portal 服务器为 office，并配置为直接认证方式。

```
[AC] interface vlan-interface 300
[AC-Vlan-interface300] portal server office method direct
```

# 在接口 VLAN 300 上启用 portal 认证域。

```
[AC-Vlan-interface300] portal domain office
[AC-Vlan-interface300] quit
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 和 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk, 禁止 VLAN 1 报文通过, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 RADIUS 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

### 3.4.3 RADIUS 服务器的配置



下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.2(E0401)、iMC UAM 5.2(E0402)），说明 RADIUS 服务器的基本配置。

---

# 增加接入设备。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[用户接入管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置认证及计费的端口号分别为“1812”和“1813”；
- 设置与 AC 交互报文时使用的认证、计费共享密钥和确认共享密钥为“admin”；

- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 100.100.1.1 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

业务 >> 用户接入管理 >> 接入设备管理 >> 接入设备配置 >> 增加接入设备

接入配置

认证端口

1812

共享密钥

\*\*\*\*\*

接入区域

无

接入设备类型

H3C(General)

业务分组

未分组

计费端口

1813

确认共享密钥

\*\*\*\*\*

业务类型

LAN接入业务

组网方式

不启用混合组网

设备列表

选择

手工增加

全部清除

共有1条记录。

| 设备名称 | 设备IP地址      | 设备型号 | 删除 |
|------|-------------|------|----|
|      | 100.100.1.1 |      | ✖  |

确定

取消

# 配置接入规则。

选择“业务”页签，单击导航树中的[用户接入管理/接入规则管理]菜单项，单击<增加>按钮，创建一条接入规则。

- 接入规则名输入“office”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 配置接入规则

业务 >> 用户接入管理 >> 接入规则管理 >> 增加接入规则 帮助

基本信息

接入规则名

office

业务分组

未分组

描述

授权信息

接入时段

无

下行速率

Kbps

优先级

证书认证

不启用

EAP证书认证

WAPI证书认证

认证证书类型

EAP-TLS认证

下发VLAN

分配IP地址

否

上行速率

Kbps

启用RSA认证

下发User Profile

下发用户组

下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线用户SSID

☐ 绑定接入设备序列号

☐ 启用接入MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线用户SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Windows可溶解客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔

30

自动重连次数

3

违规处理模式

下线

监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

IP地址获取方式

不限制

必须静态设置

必须动态获取

确定

取消

- # 增加服务配置。
- 选择“业务”页签，单击导航树中的[用户接入管理/服务配置管理]菜单项，进入服务器配置管理页面，在该页面中单击<增加>按钮，进入增加服务配置页面。
- 输入服务名为“office”、服务后缀为“office”；
  - 缺省接入规则输入“office”；
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 增加服务配置

业务 >> 用户接入管理 >> 服务配置管理 >> 增加服务配置

帮助

基本信息

\* 服务名

office

服务后缀

office

\* 业务分组

未分组

\* 缺省私有属性下发策略

不使用

\* 计费策略

不计费

服务描述

☒ 可申请

☐ Porta智能终端快速认证

接入策略列表

增加

| 接入场景 | 接入规则 | 私有属性下发策略 | 优先级 | 修改 | 删除 |
|------|------|----------|-----|----|----|
|------|------|----------|-----|----|----|

确定

取消

- # 增加用户配置。
- 选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户]菜单项，单击<增加>按钮，增加一个接入用户，再选择<增加用户>。
- 用户姓名输入“test”；
  - 证件号码输入“1234”；
  - 用户分组选择“未分组”；
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 增加用户配置

增加用户

基本信息

\* 用户姓名

test

\* 证件号码

1234

通讯地址

电话

电子邮件

\* 用户分组

未分组

确定

取消

- # 增加接入用户配置。
- 返回主页面，输入：
- 账号名输入“office”；
  - 密码与密码确认输入“admin”；
  - 选择服务名“office”；
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。



图6 增加接入用户

 用户 >> 所有接入用户 >> 增加接入用户

 帮助

接入用户

接入信息

用户姓名

test

选择

增加用户

帐号名

office

☐ 预开用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码

•••••

密码确认

•••••

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

失效日期

Porta智能终端最大绑定数

1

最大闲置时长

分钟

在线数量限制

1

帐号类型

预付费

预付金额

0元

自助充值

允许

登录提示信息

接入服务

|                                     | 服务名    | 服务后缀   | 状态  | 计费策略 | 分配IP地址 |
|-------------------------------------|--------|--------|-----|------|--------|
| <input checked="" type="checkbox"/> | office | office | 可申请 | User |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线用户SSID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

绑定域

IP地址

MAC地址

 提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

3.5 验证配置

# 使用 `display portal user all` 发现有 Portal 用户在线。

```
<AC> display portal user all
Index:103
State:ONLINE
SubState:NONE
ACL:NONE
MAC                IP                Vlan      Interface
0017-9a00-7cb8     100.30.1.50      300       Vlan-interface300
Total 1 user(s) matched, 1 listed.
```

# 使用命令 **display connection** 查看有用户在线。

```
<AC> display connection
Index=103 ,Username=test@office
MAC=0017-9a00-7cb8 ,IP=100.30.1.50
Total 1 connection(s) matched.
```

# 通过命令 **display connection ucibindex** 查看连接索引为 103 的用户连接的相关信息。

```
<AC> display connection ucibindex 103
Index=103 , Username=test@office
MAC=0017-9a00-7cb8
IP=100.30.1.50
Access=PORTAL ,AuthMethod=PAP
Port Type=Wireless-802.11,Port Name=N/A
Initial VLAN=300, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2013-11-06 10:54:51 ,Current=2013-11-06 10:54:59 ,Online=00h00m08s
Total 1 connection matched.
```

## 3.6 配置文件

- AC:
 

```
#
domain default enable office
#
portal server office ip 100.30.1.1
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
portal local-server http
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
network 100.100.1.0 mask 255.255.255.0
gateway-list 100.100.1.1
#
```

```

dhcp server ip-pool vlan300
 network 100.30.1.0 mask 255.255.255.0
 gateway-list 100.30.1.1
#
radius scheme office
 server-type extended
 primary authentication 100.100.1.10
 primary accounting 100.100.1.10
 primary authentication 191.100.0.10 key cipher $c$3$tdugLutQBoSpQVQvMPEBErb4UvJMsQ==
 primary accounting 191.100.0.10 key cipher $c$3$LMHLQJ/lqJZ0ZLhm7PMR8Z5hOdd9ig==
 user-name-format without-domain
#
domain office
 authentication portal radius-scheme office
 authorization portal radius-scheme office
 accounting portal radius-scheme office
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
wlan service-template 1 clear
 ssid office
 bind WLAN-ESS 1
 service-template enable
#
interface Vlan-interface100
 ip address 100.100.1.1 255.255.0.0
#
interface Vlan-interface300
 ip address 100.30.1.1 255.255.0.0
 portal server office method direct
 portal domain office
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 300
 port trunk pvid vlan 100
#
interface WLAN-ESS1
 port link-type hybrid
 port hybrid pvid vlan 200
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 mac-vlan enable
#
wlan ap officeap model WA2620E-AGN
 serial-id 21023529G007C000020

```

```

radio 1
  service-template 1 vlan 300
  radio enable
#
  dhcp enable
#
Switch:
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 100
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 采用本地 Portal 服务器与 LDAP 服务器组合对用户认证的典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |    |
|------------------------|----|
| 1 简介.....              | 1  |
| 2 配置前提 .....           | 1  |
| 3 配置举例 .....           | 1  |
| 3.1 组网需求 .....         | 1  |
| 3.2 配置注意事项.....        | 1  |
| 3.3 配置步骤.....          | 2  |
| 3.3.1 AC 的配置 .....     | 2  |
| 3.3.2 Switch 的配置 ..... | 4  |
| 3.3.3 LDAP 服务器的配置..... | 4  |
| 3.4 验证配置 .....         | 12 |
| 3.5 配置文件 .....         | 13 |
| 4 相关资料 .....           | 14 |

# 1 简介

本文档介绍在无线控制器上配置本地 Portal 服务器，通过 LDAP 协议将 AC 设备解析出的用户名和密码传到 LDAP 服务器上的组合认证方式对无线用户进行认证的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

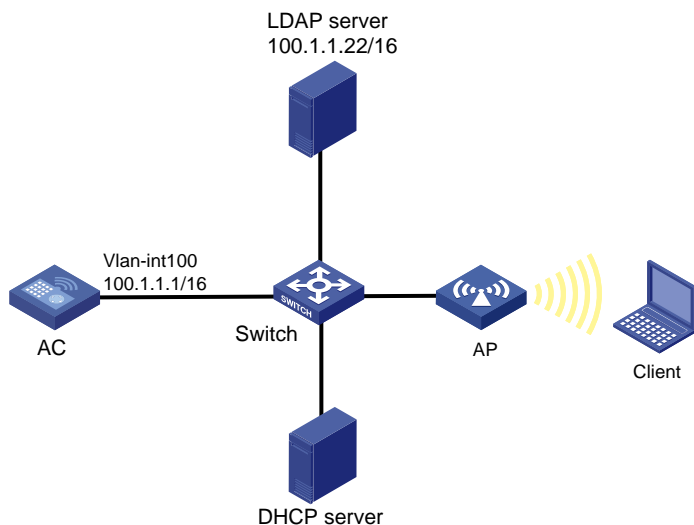
本文档假设您已了解 AAA、Portal、WLAN 特性。

## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示组网，AP 和 Client 通过 DHCP 服务器获取 IP 地址，要求：在 AC 上配置本地 Portal 服务器对 Client 推送 Portal 认证界面，并采用 LDAP 服务器对 Client 进行远程身份认证。

图1 本地 Portal 服务器与 LDAP 服务器组合认证组网图



### 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

设备缺省自带一套认证页面，如果用户需要自定义认证页面，请提前将自定义的认证页面上传到设备中，并通过 **portal local-server bind** 命令将上传的文件进行绑定，本例采用缺省认证页面。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 100.1.1.1 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口的属性为 trunk，允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 WLAN-ESS 接口

# 创建接口 WLAN-ESS 1。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 在 Hybrid 端口上使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

#### (3) 配置无线服务模板

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```



# 使能服务模板。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

#### (4) 在 AC 下绑定无线服务模板

# 创建 AP 模板，名称为 officeap，型号名称选择 WA2620E-AGN，并配置其序列号。

```
[AC] wlan ap officeap model WA2620E-AGN
```

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将服务模板 1 绑定到 AP 的 radio 2 口。

```
[AC-wlan-ap-officeap-radio-2] service-template 1
```

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

```
[AC-wlan-ap-officeap] quit
```

#### (5) 配置 LDAP 方案

# 创建 LDAP 方案。

```
[AC] ldap scheme ldap1
```

# 配置 LDAP 认证服务器的 IP 地址。

```
[AC-ldap-ldap1] authentication-server 100.1.1.22
```

# 配置具有管理员权限的用户 DN。

```
[AC-ldap-ldap1] login-dn cn=administrator,cn=users,dc=myias,dc=com
```

# 配置具有管理员权限的用户密码。

```
[AC-ldap-ldap1] login-password simple admin!123456
```

# 配置查询用户的起始目录。

```
[AC-ldap-ldap1] user-parameters search-base-dn dc=myias,dc=com
```

```
[AC-ldap-ldap1] quit
```

#### (6) 配置 Portal 认证

# 配置 ISP 域的认证方案。

```
[AC] domain dm
```

```
[AC-isp-dm] authentication default ldap-scheme ldap1
```

```
[AC-isp-dm] authorization default none
```

```
[AC-isp-dm] accounting default none
```

```
[AC-isp-dm] quit
```

# 配置本地 Portal 服务器。

```
[AC] portal server local ip 100.1.1.1
```

```
[AC] portal local-server http
```

# 在接口 VLAN 300 上使能 Portal，指定 Portal 服务器为 office，并配置为直接认证方式。

```
[AC] interface vlan-interface 300
```

```
[AC-Vlan-interface300] portal server local method direct
```

# 在接口 VLAN 300 上启用 portal 认证域。

```
[AC-Vlan-interface300] portal domain dm
```

```
[AC-Vlan-interface300] quit
```

### 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 的 GigabitEthernet1/0/1 接口的属性为 trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

### 3.3.3 LDAP 服务器的配置



说明

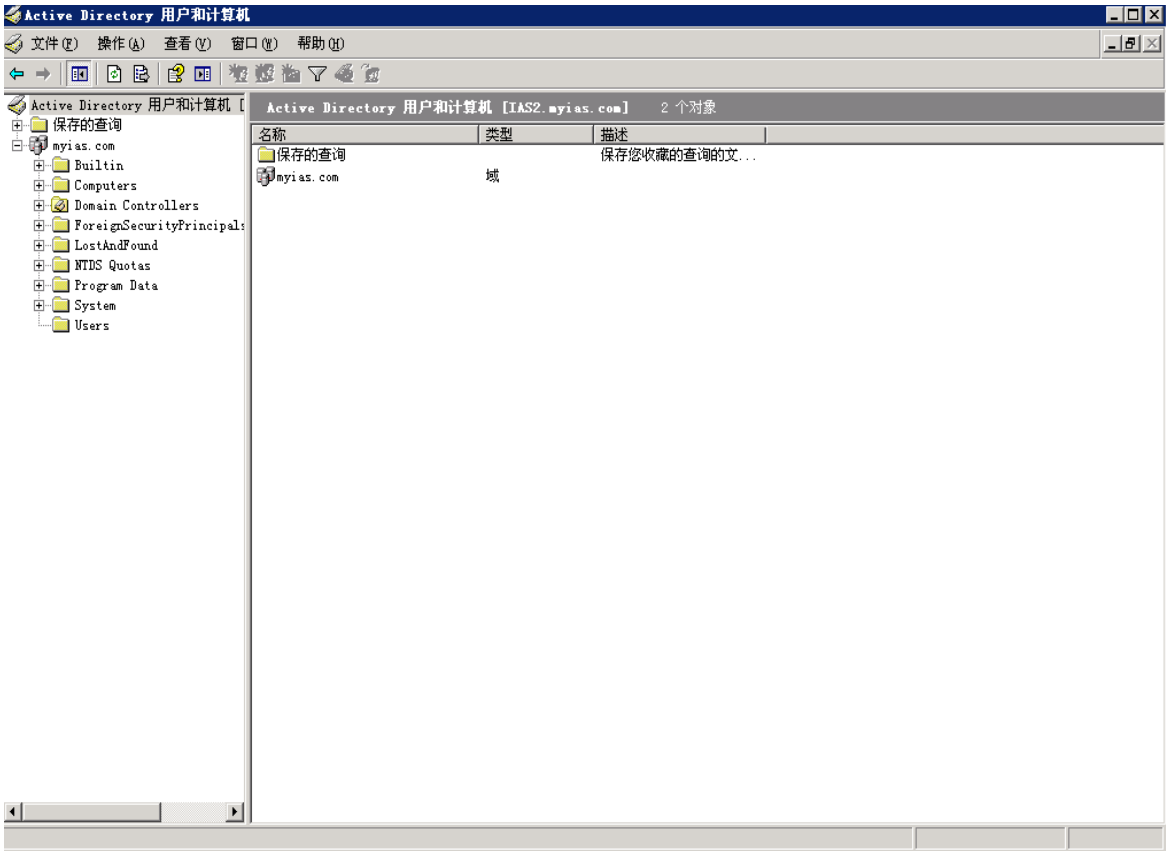
本文以 Microsoft Windows 2003 Server 的 Active Directory 为例, 说明该例中 LDAP 服务器的基本配置。

---

(1) 添加用户 aa

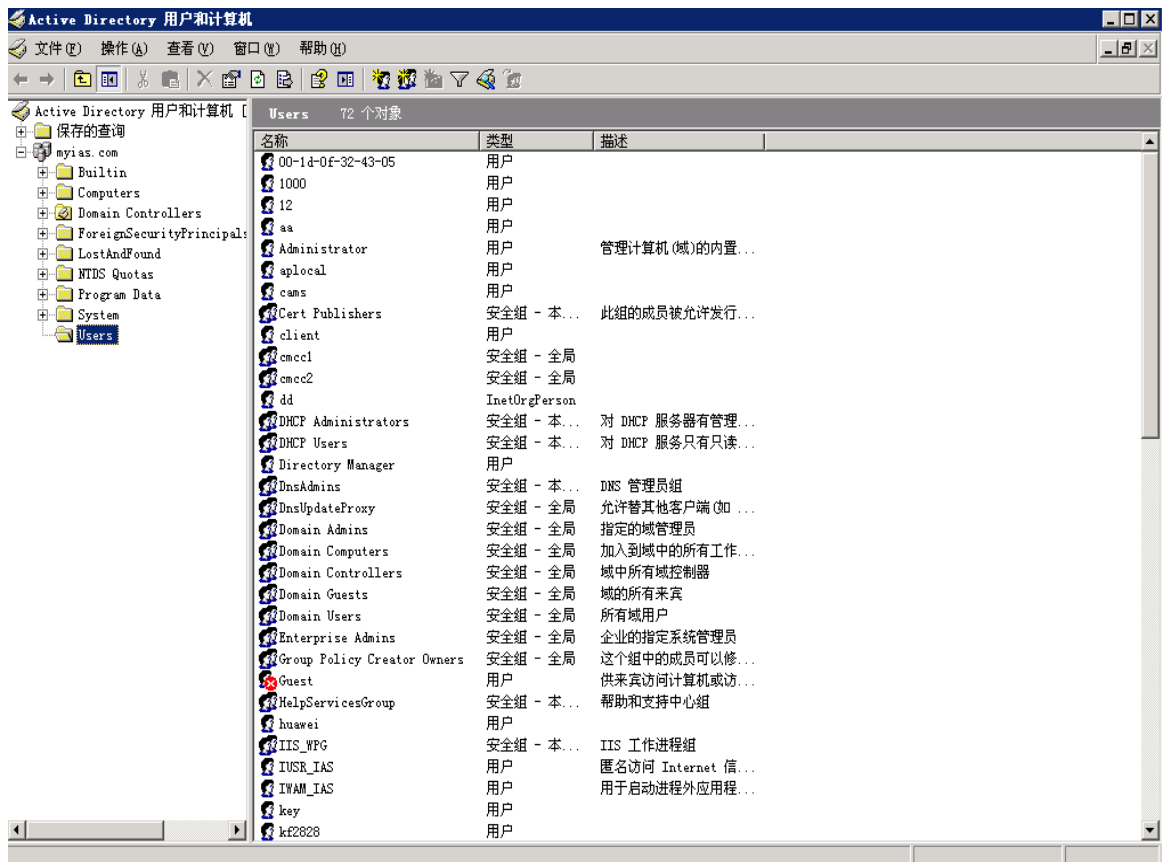
# 在 LDAP 服务器上, 选择[开始/管理工具]中的[Active Directory 用户和计算机], 打开 Active Directory 用户管理界面。

图2 打开 Active Directory 用户管理界面



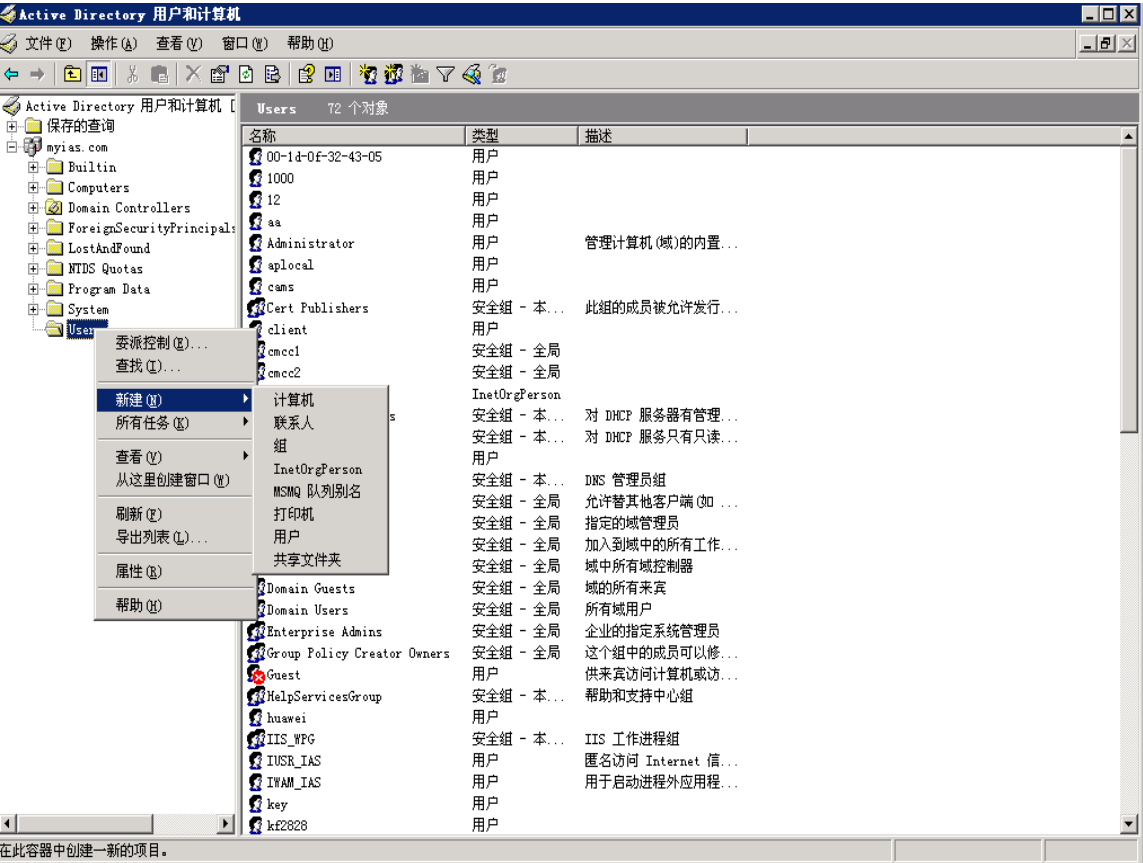
# 在 Active Directory 用户管理界面的左侧导航树中，点击 myias.com 节点下的<Users>按钮。

图3 添加用户



# 右键单击“Users”，选择[新建/用户]，打开“新建对象-用户”对话框。

图4 新建用户



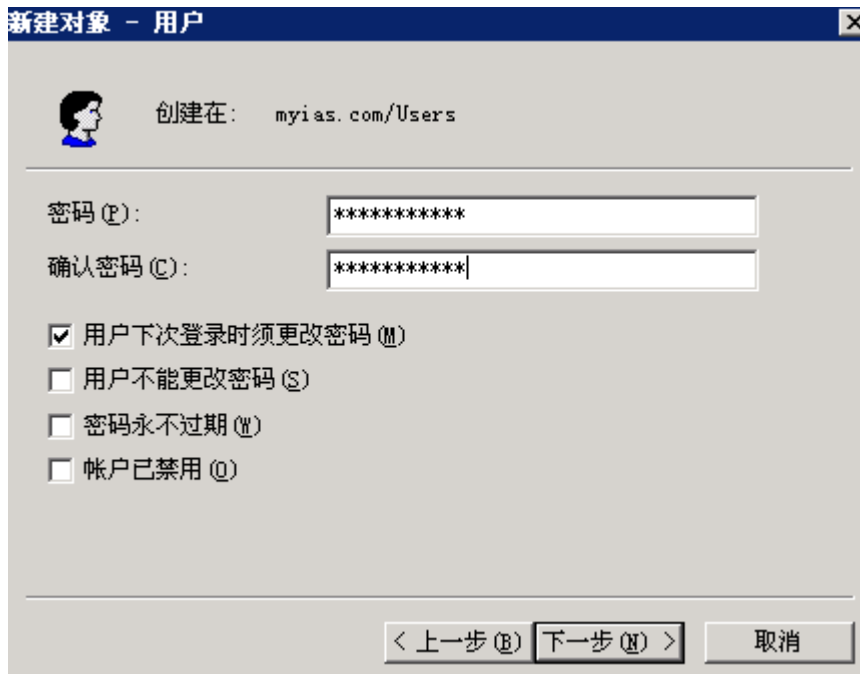
# 在对话框中输入用户信息和用户登录名 aa，并单击<下一步>按钮。

图5 新建用户 aa



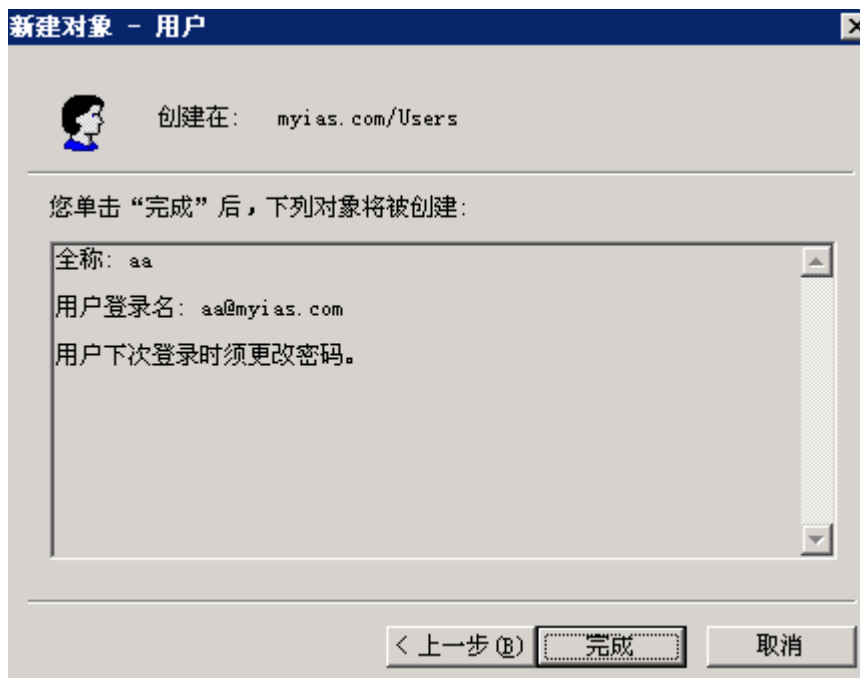
# 在弹出的对话框内输入密码，并确认密码，然后单击<下一步>按钮。

图6 设置用户密码



# 完成新建用户。

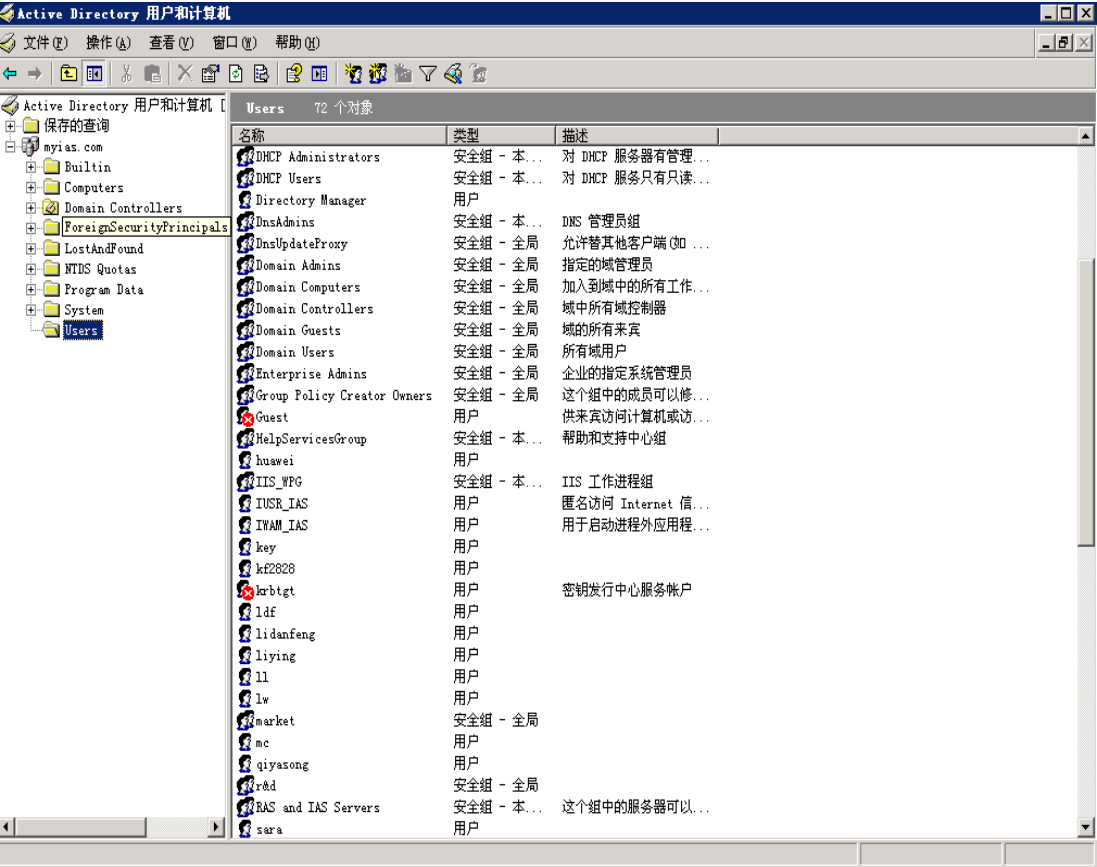
图7 完成新建用户



(2) 将用户 aa 加入 Users 组

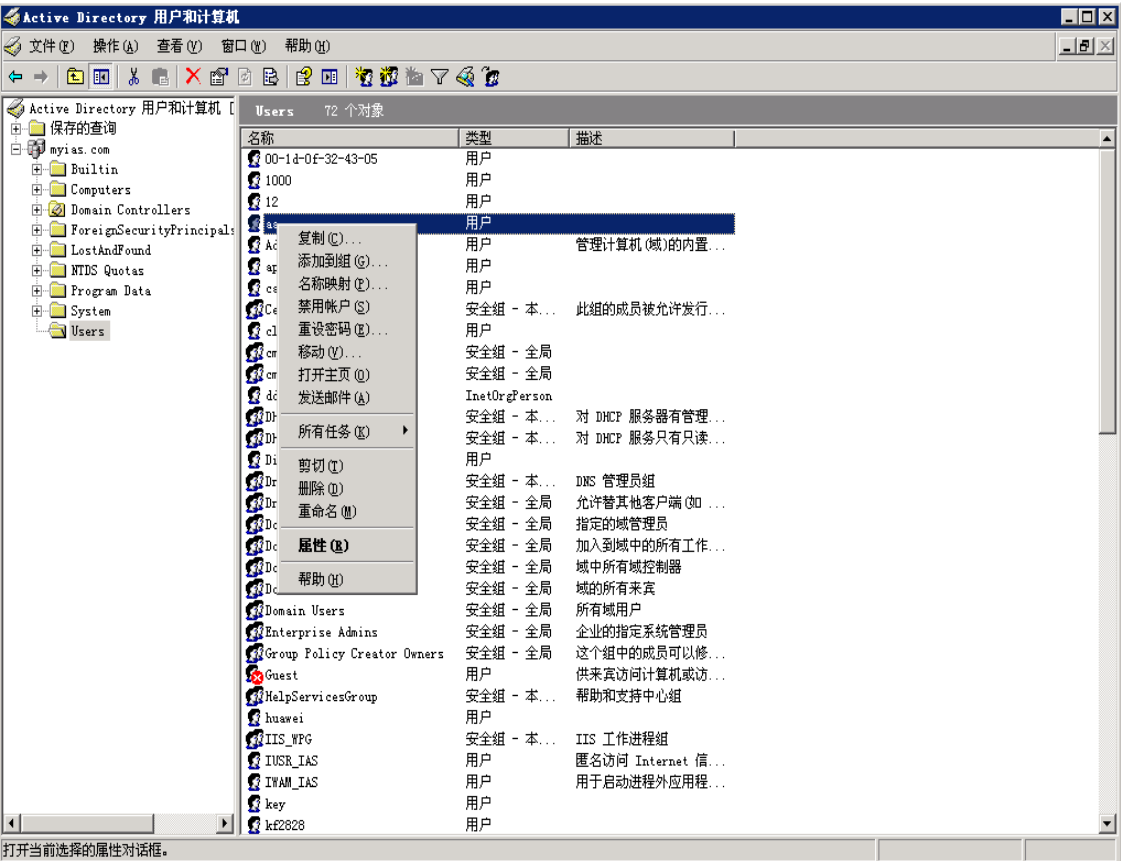
# 在 Active Directory 用户管理界面的左侧导航树中，单击 myias.com 节点下的“Users”按钮。

图8 将用户加入组



# 在右侧的 Users 信息框中右键单击用户 aa，选择“属性”项。

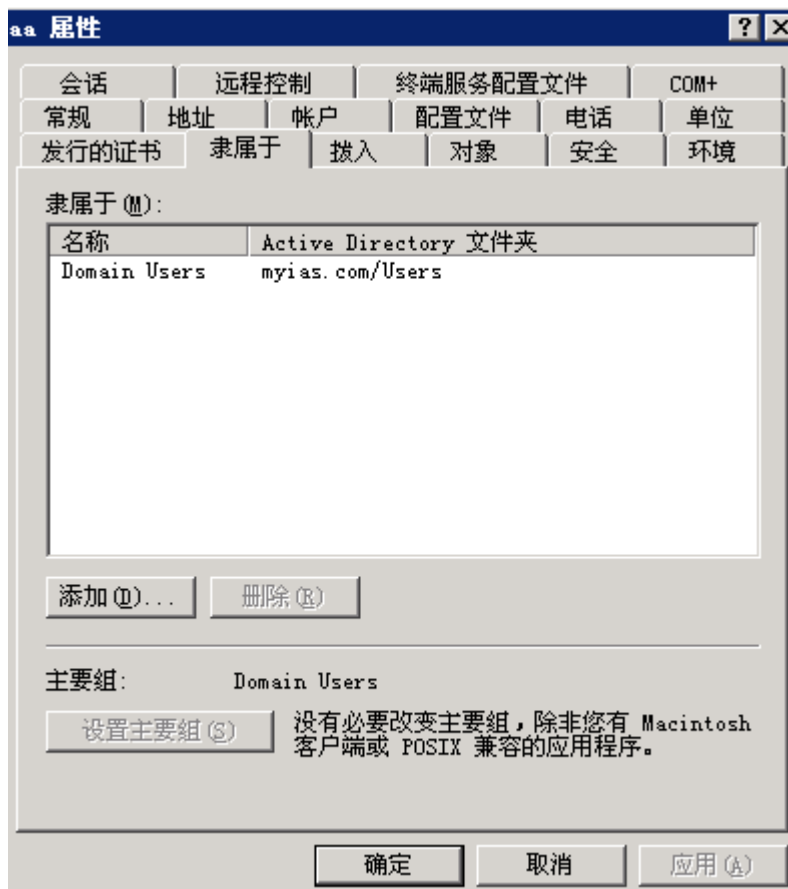
图9 选择用户



# 选择“隶属于”页签，并单击<添加(D)...>按钮。

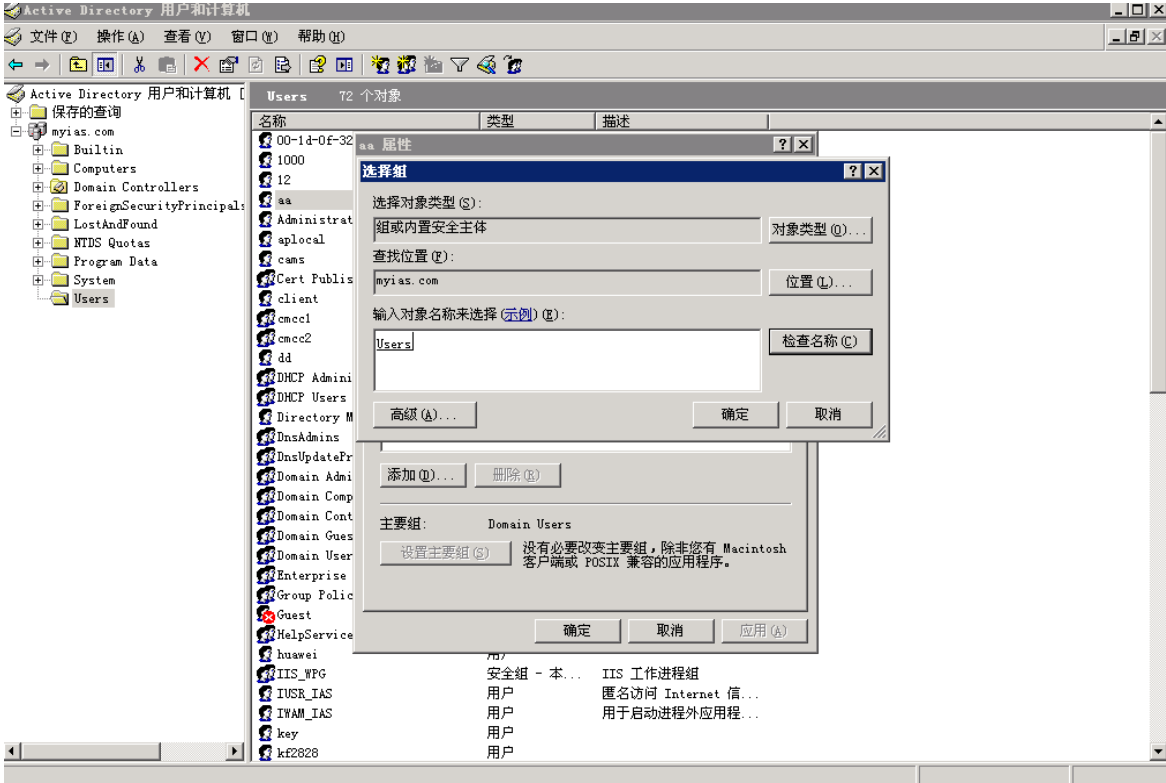


图10 修改用户属性



# 在弹出的[选择组]对话框中的可编辑区域框中输入对象名称“Users”，单击<确定>，完成用户 aa 添加到 Users 组。

图11 添加用户 aa 到用户组 Users



# 完成用户 aa 的添加之后，还需要配置管理员用户 administrator 的密码。

- 在右侧的 Users 信息框中右键单击管理员用户 administrator，选择“设置密码(S)...”项；
- 在弹出的密码添加对话框中设置管理员密码。

### 3.4 验证配置

# Client 关联到 ssid: service，此时 Client 会自动获取 100.1.0.0/16 网段的地址。

打开 Client 上的 IE 浏览器，输入任意的 IP 地址，按回车，网页会自动跳转到 Portal 认证页面，输入用户名: rd\_user，密码:ldap!123456，鼠标点击 login 按钮，认证成功。

# 用户通过认证后，在 AC 上使用命令 **display portal user all** 可以查看到有 Portal 用户在线。

```
<AC> display portal user all
Index:17
State:ONLINE
SubState:NONE
ACL:3777
Work-mode:stand-alone
MAC                IP                Vlan    Interface
-----
2477-0341-f118     100.1.1.2         2       Vlan-interface100
Total 1 user(s) matched, 1 listed.
```

## 3.5 配置文件

- AC:

```
#
portal server local ip 100.1.1.1
portal local-server http
#
vlan 100
#
vlan 200
#
vlan 300
#
ldap scheme ldap1
authentication-server 100.1.1.22
login-dn cn=administrator,cn=users,dc=myias,dc=com
login-password cipher $c$3$jgaNCoF0GQMYgxyJP6/zxYldQwOYeJSzI9uv6JEO4Q==
user-parameters search-base-dn dc=myias,dc=com
#
domain dm
authentication default ldap-scheme ldap1
authorization default none
accounting default none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200 300
#
interface Vlan-interface100
ip address 100.1.1.1 255.255.0.0
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
```

```
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
  radio 1
  radio 2
    service-template 1
    radio enable
#
•   Switch:
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 100 300
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
  poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# PSK 认证方式典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 1 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 3 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 5 |
| 4 相关资料 .....           | 6 |

# 1 简介

本文介绍了 AC PSK 特性的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 安全特性。

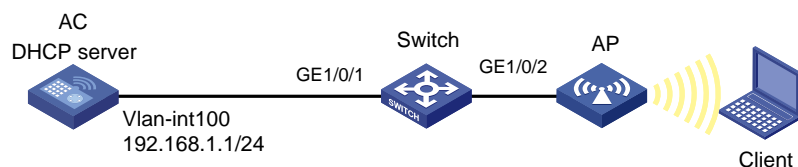
## 3 配置举例

### 3.1 组网需求

如图 1 所示，AP 通过交换机与 AC 相连，具体应用需求如下：

- AC 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址；
- 使用 PSK 认证方式对客户端进行身份认证。

图1 PSK 认证组网图



### 3.2 配置思路

为实现 PSK 认证方式对客户端进行身份认证，配置无线端口 WLAN-ESS1 的端口安全模式为 PSK。

### 3.3 配置注意事项

- 采用 PSK 加密方式时接入无线链路认证方式必须为开放式系统认证。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。同时 VLAN100 为无线用户接入的 VLAN。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.1 24
[AC-Vlan-interface100] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，当前 Trunk 口的 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 DHCP 功能

# 全局下使能 DHCP。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 1 为 AP 和 Client 动态分配的网段为 192.168.1.0/24，网关地址为 192.168.1.1。

```
[AC] dhcp server ip-pool 1
[AC-dhcp-pool-1] network 192.168.1.0 24
[AC-dhcp-pool-1] gateway-list 192.168.1.1
[AC-dhcp-pool-1] quit
```

#### (3) 配置端口安全。

# 使能端口安全功能。

```
[AC] port-security enable
```

# 创建编号为 1 的 WLAN-ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 100，禁止 VLAN 1 通过并允许 VLAN 100 不带 tag 通过。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 100
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 100 untagged
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

# 配置端口安全模式为 PSK。

```
[AC-WLAN-ESS1] port-security port-mode psk
```



```

# 在接口 WLAN-ESS1 下使能 11key 类型的密钥协商功能。
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 在接口 WLAN-ESS1 下配置预共享密钥为 12345678。
[AC-WLAN-ESS1] port-security preshared-key pass-phrase 12345678
[AC-WLAN-ESS1] quit
(4) 配置无线服务模板。
# 创建 crypto 类型的无线服务模板 1。
[AC] wlan service-template 1 crypto
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 设置无线客户端接入该无线服务（SSID）的认证方式为开放式系统认证。
[AC-wlan-st-1] authentication-method open-system
# 使能 TKIP 加密套件。
[AC-wlan-st-1] cipher-suite tkip
# 配置信标和探查帧携带 WPA IE 信息。
[AC-wlan-st-1] security-ie wpa
# 使能服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(5) 在 AC 上配置 AP 并绑定无线服务。
# 创建一个 AP 管理模板，其名称为 officeap1，型号名称为 WA2620E-AGN。
[AC] wlan ap officeap1 model WA2620E-AGN
# 设置 AP 的序列号。
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
# 进入 AP 的 radio1 射频视图，配置服务模板与射频 1 进行关联，使能 AP 的 radio 1 射频。
[AC-wlan-ap-officeap1] radio 1
[AC-wlan-ap-officeap1-radio-1] service-template 1
[AC-wlan-ap-officeap1-radio-1] radio enable
[AC-wlan-ap-officeap1-radio-1] return

```

### 3.4.2 Switch 的配置

```

# 创建 VLAN 100，用于转发 AC 和 AP 间 LWAPP 隧道内的流量和无线用户的接入。
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，禁止 VLAN 1 通过，配置 PVID 为 100，允许 VLAN 100 通过。
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100

```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

## 3.5 验证配置

- (1) 在配置错误预共享密钥的情况下，Client 不能访问 Internet 上的资源。
- (2) 在配置正确预共享密钥的情况下，通过命令 **display wlan client verbose** 看到 Client 可以成功关联，并且可以正常访问 Internet 上的资源。

```
[AC] display wlan client verbose
```

```
Total Number of Clients          : 1
```

```
Client Information
```

```
-----
MAC Address          : 80f6-2eba-3330
User Name            :
IP Address           : 192.168.1.2
AID                  : 252
AP Name              : officeap1
Radio Id             : 2
Antenna Id           : 0
Service Template Number : 1
SSID                 : service
BSSID                : 00ef-1234-5612
Port                 : WLAN-DBSS1:16269
VLAN                  : 100
State                : Running
Power Save Mode      : Active
Wireless Mode        : 11gn
QoS Mode             : WMM
Listen Interval (Beacon Interval) : 0
RSSI                 : 56
Rx/Tx Rate           : 1/1
Client Type          : WPA
Authentication Method : Open System
Authentication Mode   : Central
AKM Method           : PSK
Key Derivation        : SHA1
4-Way Handshake State : PTKINITDONE
Group Key State       : REKEYESTABLISHED
Encryption Cipher     : TKIP
PMF Status            : -NA-
Roam Status           : Normal
```

```
Roam Count          : 0
Up Time (hh:mm:ss)  : 01:06:48
```

---

## 3.6 配置文件

- AC

```
#
vlan 100
#
port-security enable
#
dhcp server ip-pool 1
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.1
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 1
authentication-method open-system
cipher-suite tkip
security-ie wpa
service-template enable
#
interface Vlan-interface100
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk pvid vlan 100
port trunk permit vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 100 untagged
port hybrid pvid vlan 100
mac-vlan enable
port-security port-mode psk
port-security tx-key-type 11key
port-security preshared-key pass-phrase 12345678
#
wlan ap officeap1 model WA2620E-AGN
serial-id 21023529G007C000020
radio 1 type 11g
channel 1
max-power 3
```

```

    service-template 1
    radio enable
#
    dhcp enable
#
    • Switch
#
    vlan 100
#
    interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100
    port trunk pvid vlan 100
#
    interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 100
    poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# AP 本地认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                           |    |
|---------------------------|----|
| 1 简介.....                 | 1  |
| 2 配置前提 .....              | 1  |
| 3 配置举例 .....              | 1  |
| 3.1 组网需求 .....            | 1  |
| 3.2 配置思路 .....            | 2  |
| 3.3 配置注意事项 .....          | 2  |
| 3.4 配置步骤 .....            | 2  |
| 3.4.1 配置 AC .....         | 2  |
| 3.4.2 Router A 的配置 .....  | 4  |
| 3.4.3 Router B 的配置 .....  | 4  |
| 3.4.4 RADIUS 服务器的配置 ..... | 5  |
| 3.5 验证配置 .....            | 10 |
| 3.6 配置文件 .....            | 11 |
| 4 相关资料 .....              | 13 |

# 1 简介

本文档介绍 AP 本地认证典型配置举例。

# 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 接入特性。

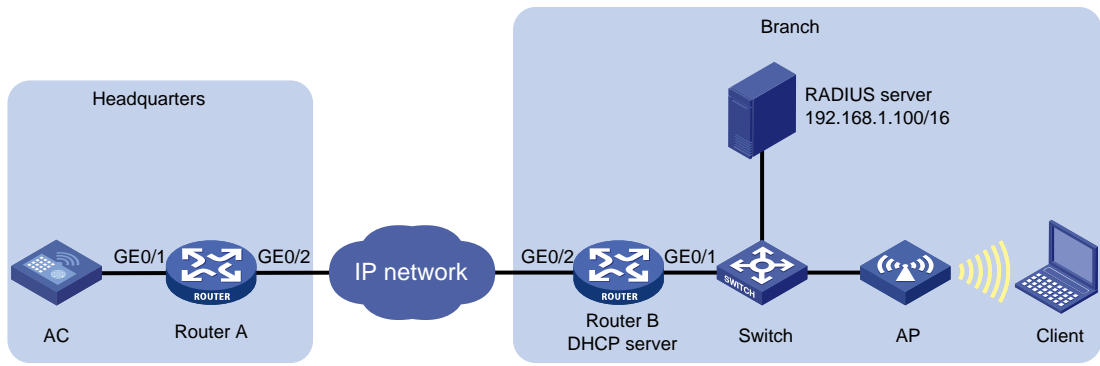
# 3 配置举例

## 3.1 组网需求

如图 1 所示，某公司将 AC 部署在总部实现对分支机构无线网络的统一管理，总部通过 VPN 与分支机构跨公网进行业务互通，分支机构本地使用 AP 作为认证实体对客户端进行认证，该公司拥有两个公网地址，其中 202.38.0.1 分给总部，202.38.0.2 分给分支机构，具体要求如下：

- 无论 AP 和 AC 正常连接或是连接出现故障时，都使用 Local 认证模式对分支机构的客户端进行 802.1X 认证。
- 将认证服务器部署在 AP 侧，保证分支机构和总部之间的网络通信出现故障时，已接入的 802.1X 客户端不会下线，可以继续访问本地资源。
- 由分支机构的网关 Router B 作为 DHCP server 为 AP 和 Client 分配 IP 地址。

图1 AP 本地认证组网图



| 设备       | 接口          | IP地址             | 设备       | 接口    | IP地址           |
|----------|-------------|------------------|----------|-------|----------------|
| AC       | Vlan-int100 | 182.100.1.100/16 | Router B | GE0/1 | 192.168.1.1/24 |
|          | Vlan-int200 | 182.200.1.100/16 |          | GE0/2 | 202.38.0.2/24  |
| Router A | GE0/1       | 182.100.1.1/24   |          |       |                |
|          | GE0/2       | 202.38.0.1/24    |          |       |                |

## 3.2 配置思路

- 在本地 PC 上编辑 AP 配置文件，并保存为 txt 文档格式，上传到 AC 的存储器上，AC 与 AP 建立 LWAPP 隧道正常连接之后，会将 AP 配置文件下发到 AP。
- 由于总部与分支机构跨公网进行通信，因此需要在总部和分支机构的网关路由器分别配置 NAT 功能，实现公网地址与私网地址的转换。
- 在 RADIUS server 上配置 AP 为接入认证设备。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 本地认证功能是 Remote AP 功能的增强，所以要本地认证功能生效，必须要保证 Remote AP 已经开启。
- 编辑 AP 配置文件时需注意，如果文件的某个命令行后面有 Tab 键，或者大量空格时，就会出现该行配置无法生效的情况。

## 3.4 配置步骤

### 3.4.1 配置 AC

- (1) 使用文本文档编辑 AP 的配置文件，将配置文件命名为 map.txt，并将配置文件上传到 AC 存储介质上。配置文件内容和格式如下：

```
port-security enable
vlan 200
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 200 tagged
port hybrid vlan 1 untagged
dot1x authentication-method eap
radius scheme imc
primary authentication 192.168.1.100
primary accounting 192.168.1.100
key authentication simple 123456
key accounting simple 123456
user-name-format without-domain
domain system
authentication default radius-scheme imc
authorization default radius-scheme imc
accounting default radius-scheme imc
```

- (2) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
```



```

[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 182.100.1.100 16
[AC-Vlan-interface100] quit
# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该
接口配置 IP 地址。
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 182.200.1.100 16
[AC-Vlan-interface200] quit
(3) 配置无线服务和认证
# 创建 WLAN-ESS 接口 1，并进入该接口视图。
[AC] interface wlan-ess 1
# 在 WLAN-ESS 接口 1 上配置 802.1X 用户的强制认证域 system，注意这里的强制认证域必须和
AP 配置文件中创建的 ISP 域保持一致。
[AC-WLAN-ESS1] dot1x mandatory-domain system
# 配置端口安全模式为 userlogin-secure-ext，并使能端口 11key 类型的密钥协商功能。
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 关闭 802.1X 多播触发功能和在线用户握手功能。
[AC-WLAN-ESS1] undo dot1x multicast-trigger
[AC-WLAN-ESS1] undo dot1x handshake
# 配置端口的链路类型为 Hybrid。
[AC-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
# 使能接口的 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
# 创建服务模板 1（加密类型服务模板），配置 SSID 为 local1x，加密方式为 AES-CCMP。
[AC] wlan service-template 1 crypto
[AC-wlan-st-1] ssid local1x
[AC-wlan-st-1] bind WLAN-ESS 1
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
# 配置使用 Local 认证模式。
[AC-wlan-st-1] authentication-mode local
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
# 创建型号为 WA2620E-AGN 的 AP 模板名为 ap1，指定其序列号为 21023529G007C000020。
[AC] wlan ap ap1 model WA2620E-AGN

```

```
[AC-wlan-ap-ap1] serial-id 21023529G007C000020
# 开启 Remote AP 功能。
[AC-wlan-ap-ap1] hybrid-remote-ap enable
# 将配置文件 map.txt 绑定到 ap1。
[AC-wlan-ap-ap1] map-configuration map.txt
# 将服务模板 1 绑定到 AP 1 的 radio 2 口。
[AC-wlan-ap-ap1] radio 2 type dot11gn
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

### 3.4.2 Router A 的配置

#### (1) 配置 Router A 接口

```
<RouterA> system-view
[RouterA] interface gigabitethernet 0/1
[RouterA-GigabitEthernet0/1] ip address 182.100.1.1 24
[RouterA-GigabitEthernet0/1] quit
[RouterA] interface gigabitethernet 0/2
[RouterA-GigabitEthernet0/2] ip address 202.38.0.1 24
[RouterA-GigabitEthernet0/2] quit
```

#### (2) 配置 NAT 功能

```
# 配置一对一静态地址转换映射。
[RouterA] nat static 182.100.1.1 202.38.0.1
# 配置的静态地址转换在接口 GigabitEthernet0/2 上生效。
[RouterA] interface gigabitethernet 0/2
[RouterA-GigabitEthernet0/2] nat outbound static
[RouterA-GigabitEthernet0/2] quit
```

### 3.4.3 Router B 的配置

#### (1) 配置 Router B 的接口

```
<RouterB> system-view
[RouterB] interface gigabitethernet 0/1
[RouterB-GigabitEthernet0/1] ip address 192.168.1.1 24
[RouterB-GigabitEthernet0/1] quit
[RouterB] interface gigabitethernet 0/2
[RouterB-GigabitEthernet0/2] ip address 202.38.0.2 24
[RouterB-GigabitEthernet0/2] quit
```

#### (2) 配置 DHCP 服务器

```
# 使能 DHCP 功能
[RouterB] dhcp enable
# 创建名为 vlan100 的 DHCP 地址池，配置地址池动态分配的网段为 192.168.1.0/24，网关地址为 192.168.1.1，为 AP 和 Client 分配 IP 地址。
[RouterB] dhcp server ip-pool vlan100 extended
```

```
[RouterB-dhcp-pool-vlan100] network 192.168.1.0 mask 255.255.255.0
[RouterB-dhcp-pool-vlan100] gateway-list 192.168.1.1
[RouterB-dhcp-pool-vlan100] quit
```

### (3) 配置 NAT 功能

# 配置 ACL 2000，仅允许对 192.168.1.0/24 网段的用户报文进行地址转换。

```
[RouterB] acl number 2000
[RouterB-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[RouterB-acl-basic-2000] quit
```

# 创建地址组 1。

```
[RouterB] nat address-group 1
```

# 添加地址组成员 202.38.0.2。

```
[RouterB-nat-address-group-1] address 202.38.0.2 202.38.0.2
[RouterB-nat-address-group-1] quit
```

# 在接口 GigabitEthernet0/2 上配置入方向动态地址转换，允许使用地址组 1 中的地址对内网访问外网的报文进行源地址转换，并在转换过程中使用端口信息。

```
[RouterB] interface gigabitethernet 0/2
[RouterB-GigabitEthernet0/2] nat inbound 2000 address-group 1
```

# 在接口 GigabitEthernet0/2 上配置出方向动态地址转换，允许使用地址组 1 中的地址对内网访问外网的报文进行源地址转换，并在转换过程中使用端口信息。

```
[RouterB-GigabitEthernet0/2] nat outbound 2000 address-group 1
[RouterB-GigabitEthernet0/2] quit
```

## 3.4.4 RADIUS 服务器的配置



说明

下面以 iMC 为例(使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202))，说明 RADIUS 服务器的基本配置。

# 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入“接入设备配置”页面，在该页面中单击<增加>按钮，进入“增加接入设备”页面。

- 设置与 AP 交互报文时使用的认证、计费共享密钥为“123456”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 在设备列表中，单击<手工增加>按钮，添加接入设备 AP 的 IP 地址为 192.168.1.2（可以在 AC 上通过 **display wlan ap address** 命令查看）；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \*1812

计费端口 \*1813

组网方式不启用混合组网

业务类型LAN接入业务

接入设备类型H3C(General)

接入设备分组无

共享密钥 \*.....

确认共享密钥 \*.....

业务分组未分组

设备列表

选择手工增加全部清除

| 设备名称 | 设备IP地址      | 设备型号 | 备注 | 删除 |
|------|-------------|------|----|----|
|      | 192.168.1.2 |      |    |    |

共有1条记录。

确定取消

- #增加接入策略。
- 选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入“接入策略配置”页面，在该页面中单击<增加>按钮，进入“增加接入策略”页面。
- 输入接入策略名“dot1x auth”；
  - 业务分组“未分组”；
  - 证书认证选择所需要认证的类型；
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

帮助

基本信息

接入策略名 \*

dot1x auth

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☐ 不启用 ☒ EAP证书认证 ☐ WAP证书认证

认证证书类型

EAP-PEAP认证

认证证书子类型

MS-CHAPV2认证

下发VLAN

下发用户组

☐ 下发User Profile

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 禁用Windows可溶解客户端

自动重连间隔(分钟) 30

自动重连次数 3

☐ 网络故障时自动重连

违规处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式

☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定

取消

# 增加接入服务配置。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入“接入服务配置”页面，在该页面中单击<增加>按钮，进入“增加接入服务”页面。

- 输入服务名“dot1x auth”；
- 业务分组“未分组”；
- 缺省接入策略“dot1x auth”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

基本信息

服务名 \*

dot1x auth

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

dot1x auth

缺省私有属性下发策略 \*

不使用

计费策略 \*

不计费

缺省BYOD页面 \*

PC-缺省页面 (PC)

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入“接入用户列表”页面，在该页面中单击<增加>按钮，进入“增加接入用户”页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“admin”；
- 输入证件号码“12345”；
- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图5 增加用户

增加用户

基本信息

用户姓名 \*

admin

证件号码 \*

12345

检查是否可用

通讯地址

电话

电子邮件

用户分组 \*

未分组

确定

取消

- 输入账号名“localuser”；
- 输入密码“123456”；
- 在接入服务处选择“dot1x auth”；
- 其他配置保持默认；
- 单击<确定>按钮完成操作。

图6 增加接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

admin

选择

增加用户

帐号名 \*

localuser

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

时

失效时间

时

最大闲置时长(分钟)

在线数里限制

1

帐号类型

预付费

预付金额(元) \*

0

自助充值

允许

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                            | 服务后缀 | 状态  | 计费策略 | 分配IP地址 |
|------------------------------------------------|------|-----|------|--------|
| <input checked="" type="checkbox"/> dot1x auth |      | 可申请 | 不计费  |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线SSID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

IP地址

MAC地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

## 3.5 验证配置

- 无论 AP 和 AC 正常连接或是连接出现故障时，都使用 Local 认证模式对分支机构的客户端进行远程 802.1X 认证。当 AP 和 AC 正常连接，在 AC 上使用命令 **display wlan client verbose**，显示信息中 **authentication-mode** 字段显示 Local，表示由 AP 作为认证实体对该客户端进行认证。

```
[AC] display wlan client verbose
```

```
Total Number of Clients      : 1
```

```
Client Information
```

```
-----
MAC Address                  : 2477-0341-da70
User Name                    : localuser
IP Address                   : 182.200.0.2
AID                          : 1
AP Name                      : ap1
Radio Id                    : 2
Antenna Id                  : 0
Service Template Number     : 1
SSID                        : local1x
BSSID                       : d4c9-efe4-e330
Port                        : WLAN-DBSS1:0
VLAN                        : 200
State                       : Running
Power Save Mode             : Active
Wireless Mode               : 11gn
Channel Band-width         : 20MHz
SM Power Save Enable       : Disabled
Short GI for 20MHz         : Supported
Short GI for 40MHz         : Not Supported
LDPC                       : Not Supported
STBC TX capability         : Not Supported
STBC RX capability         : Supported
Support MCS Set             : 0,1,2,3,4,5,6,7,8,9,
                             10,11,12,13,14,15,16,17,18,19,
                             20,21,22,23
QoS Mode                   : WMM
Listen Interval (Beacon Interval) : 100
RSSI                       : 43
Rx/Tx Rate                 : 24/195
Client Type                : WPA2(RSN)
Authentication Method       : Open System
Authentication Mode         : Local
AKM Method                 : Dot1X
Key Derivation              : SHA1
4-Way Handshake State      : PTKINITDONE
Group Key State            : IDLE
```



```

Encryption Cipher          : AES-CCMP
PMF Status                 : -NA-
Roam Status                : Normal
Roam Count                 : 0
Up Time (hh:mm:ss)        : 00:00:50

```

---

- 由于客户端使用AP本地认证上线，所以在AC上使用 **display connection** 命令查看客户端，不会查看到客户端信息。

```

[AC] display connection
Total 0 connection(s) matched.

```

## 3.6 配置文件

- AC:

```

#
port-security enable
#
vlan 100
#
vlan 200
#
wlan service-template 1 crypto
ssid locallx
bind WLAN-ESS 1
cipher-suite ccmp
security-ie rsn
authentication-mode local
service-template enable
#
interface Vlan-interface1
ip address 8.182.1.100 255.255.0.0
#
interface Vlan-interface100
ip address 182.100.1.100 255.255.0.0
#
interface Vlan-interface200
ip address 182.200.1.100 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200

```

```

mac-vlan enable
port-security port-mode userlogin-secure-ext
port-security tx-key-type 1lkey
undo dot1x handshake
dot1x mandatory-domain system
undo dot1x multicast-trigger
#
wlan ap ap1 model WA2620E-AGN id 1
map-configuration map.cfg
serial-id 21023529G007C000020
hybrid-remote-ap enable
radio 1
radio 2
    service-template 1
    radio enable
#
ip https ssl-server-policy access-policy
ip https enable
#

```

- **Router A:**

```

#
nat static 182.100.1.1 202.38.0.1
#
interface GigabitEthernet0/1
port link-type route
ip address 182.100.1.1 255.255.255.0
#
interface GigabitEthernet0/2
port link-type route
ip address 202.38.0.1 255.255.255.0
nat outbound static
#

```

- **Router B:**

```

#
dhcp enable
#
dhcp server ip-pool vlan100 extended
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.1
#
interface GigabitEthernet0/1
port link-type route
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/2
port link-type route
ip address 202.38.0.2 255.255.255.0
nat outbound 2000 address-group 1

```

```
nat inbound 2000 address-group 1
#
acl number 2000
rule permit source 192.168.1.0 0.0.0.255
#
nat address-group 1
address 202.38.0.2 202.38.0.2
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“三层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“三层技术命令参考”。

# SSH 接入 Password 认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤.....          | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 4 |
| 3.4 验证配置 .....         | 5 |
| 3.5 配置文件 .....         | 7 |
| 4 相关资料 .....           | 9 |

# 1 简介

本文档介绍了 SSH 接入 Password 认证配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

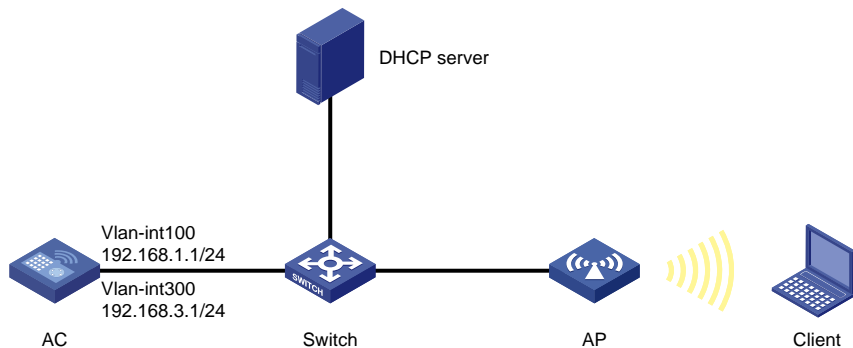
本文档假设您已了解 SSH 特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 作为 Stelnet 服务器，并采用 password 认证方式对无线客户端 Client 进行认证，Client 的用户名和密码保存在 AC 本地，使 Client 可以安全的登录到 AC 上，且 Client 的用户级别为管理级。

图1 无线控制器作为 Stelnet 服务器配置组网图



### 3.2 配置注意事项

- 由于不同客户端支持的公钥算法不同，为了确保所有的无线客户端都能够成功登录 AC，需要在 AC 上同时生成 DSA 和 RSA 两种密钥对。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.1 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 192.168.3.1 24
[AC-Vlan-interface300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 300 的报文通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS 1 接口，并设置端口的链路类型为 Hybrid。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

#### (2) 配置 Stelnet 服务器

# 在 AC 上生成 RSA 密钥对。

```
[AC] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
```

```

Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
+++++
+++++++
# 在 AC 上生成 DSA 密钥对。
[AC] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:512
Generating Keys...
+++++++
+++++++*
+++++++
+++++++
+++++++
+++++++
+++++++*+++
+++
# 使能 SSH 服务器功能。
[AC] ssh server enable
# 设置 Stelnet 客户端登录用户界面的认证方式为 AAA 认证。
[AC] user-interface vty 0 4
[AC-ui-vty0-4] authentication-mode scheme
# 设置 AC 上远程用户登录协议为 SSH。
[AC-ui-vty0-4] protocol inbound ssh
[AC-ui-vty0-4] quit
# 创建本地用户 client001，密码为 aabbcc，服务类型为 SSH，本地用户的级别为 3（管理级）。
[AC] local-user client001
[AC-luser-client001] password simple aabbcc
[AC-luser-client001] service-type ssh
[AC-luser-client001] authorization-attribute level 3
[AC-luser-client001] quit
# 配置 SSH 用户 client001 的服务类型为 Stelnet，认证方式为 password 认证。
[AC] ssh user client001 service-type stelnet authentication-type password
(3) 配置无线服务
# 创建 clear 类型的服务模板 1。
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```



```
[AC-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(4) 配置射频接口并绑定服务模板
# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。
[AC] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] return
```

### 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过，并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

## 3.4 验证配置



说明

Stelnet客户端软件有很多，例如PuTTY、OpenSSH等，本文中仅以客户端软件PuTTY0.58为例，说明 Stelnet 客户端的配置方法。

# 在 AC 上通过 **display local-user** 命令查看本地用户的信息，可以看到无线用户 **client001** 的服务类型为 **SSH**，且用户级别为管理级。

```
<AC> display local-user
```

```
The contents of local user admin:
```

```
State:                Active
ServiceType:          telnet
Access-limit:         Disabled          Current AccessNum: 0
User-group:           system
```

```
Bind attributes:
```

```
Authorization attributes:
```

```
User Privilege:       3
```

```
The contents of local user client001:
```

```
State:                Active
ServiceType:          ssh
Access-limit:         Disabled          Current AccessNum: 0
User-group:           system
```

```
Bind attributes:
```

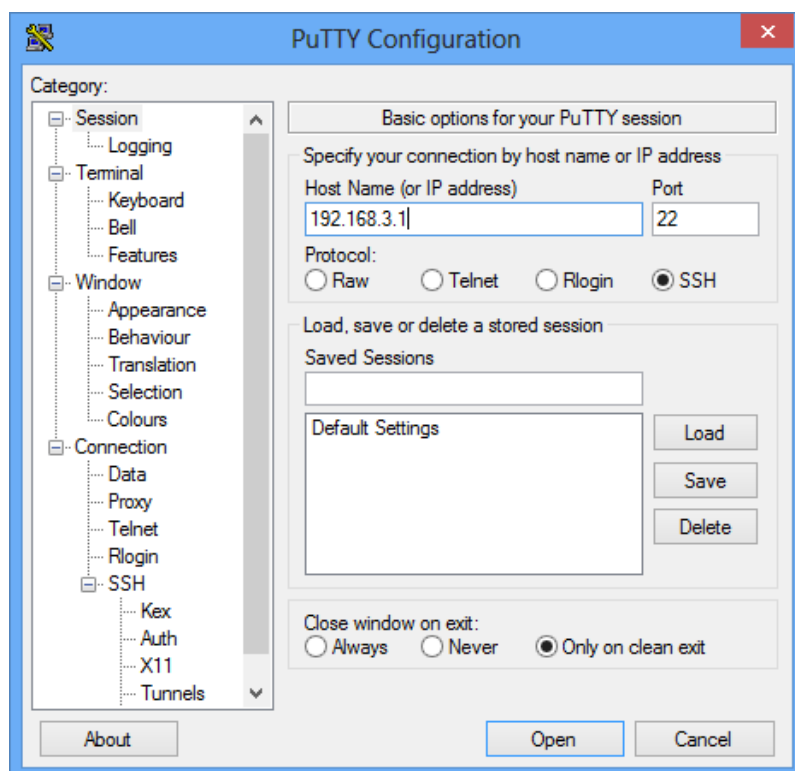
```
Authorization attributes:
```

```
User Privilege:       3
```

```
Total 2 local user(s) matched.
```

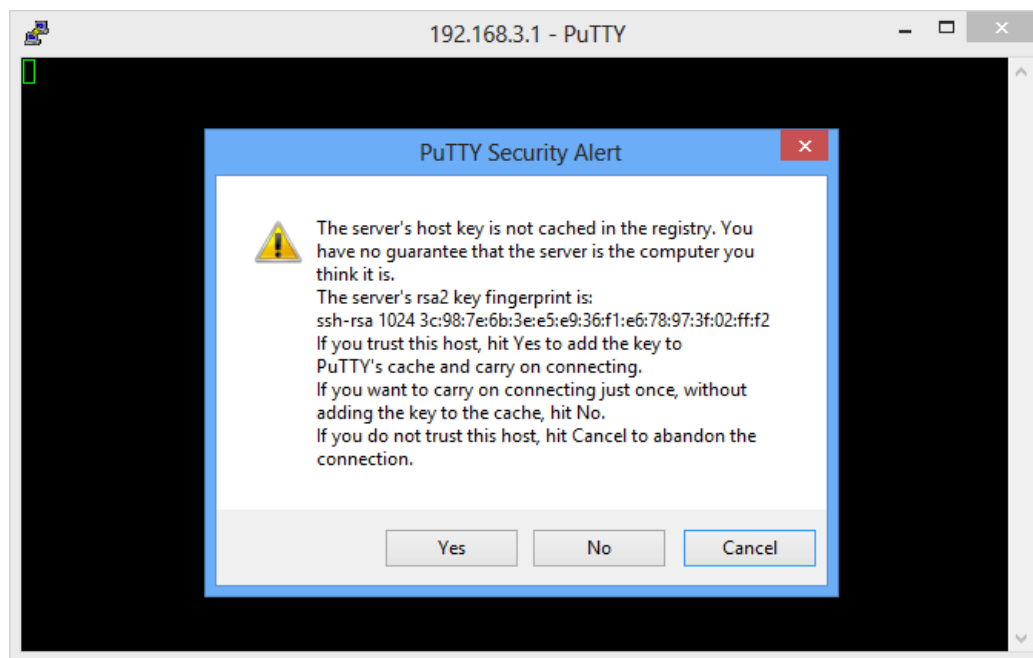
# 在 Client 上打开 PuTTY.exe 程序，出现如[图 2](#)所示的客户端配置界面。在“Host Name (or IP address)”文本框中输入 Stelnet 服务器的 IP 地址为 192.168.3.1，单击<Open>按钮。

图2 Stelnet 客户端配置界面



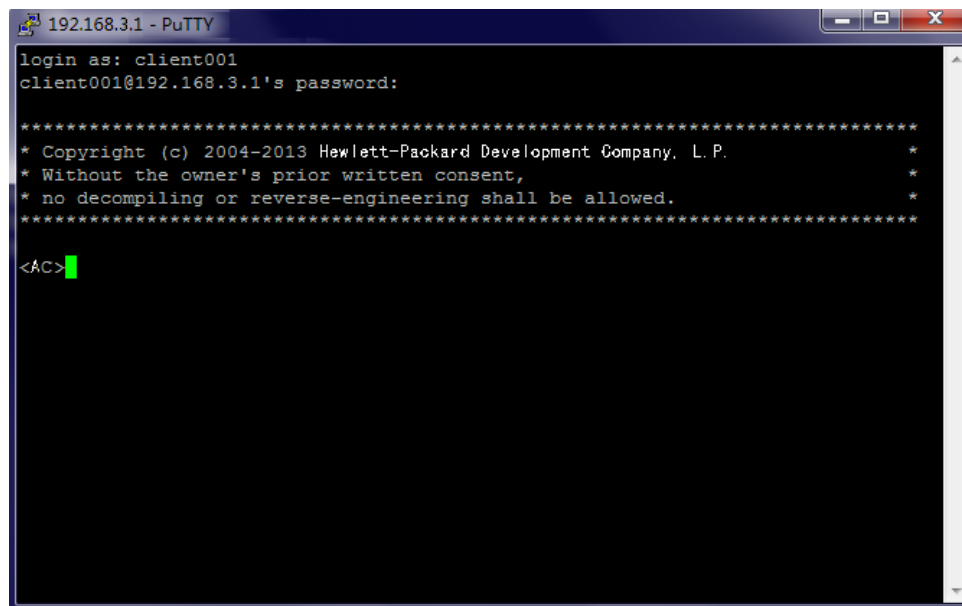
# 若首次登录，客户端会弹出警告信息如图3所示，单击<Yes>按钮。

图3 首次登录时弹出的警告信息



# 如图4所示，按提示输入用户名 client001 及密码 aabbcc，即可进入 AC 的配置界面。

图4 输入用户名和密码后登录到 AC 配置界面



# 当 Stelnet 客户端成功登录时，在 AC 上会显示用户 client001 上线的日志信息。

<AC>

#Feb 19 11:23:43:342 2014 AC SHELL/4/LOGIN:

Trap 1.3.6.1.4.1.11.2.14.11.15.2.2.1.1.3.0.1:client001 login from VTY

%Feb 19 11:23:43:362 2014 AC SHELL/5/SHELL\_LOGIN: client001 logged in from 192.168.3.5.

# 通过 **display ssh server session** 命令查看会话信息，可以看到用户 client001 已上线。

<AC> display ssh server session

| Conn  | Ver | Encry | State       | Retry | SerType | Username  |
|-------|-----|-------|-------------|-------|---------|-----------|
| VTY 0 | 2.0 | AES   | Established | 0     | Stelnet | client001 |

# 当 Stelnet 客户端退出时，在 AC 上会显示用户 client001 下线的日志信息。

<AC>

#Feb 19 11:24:17:994 2014 AC SHELL/4/LOGOUT:

Trap 1.3.6.1.4.1.11.2.14.11.15.2.2.1.1.3.0.2:client001 logout from VTY

%Feb 19 11:24:18:015 2014 AC SHELL/5/SHELL\_LOGOUT: client001 logged out from 192.168.3.5.

# 通过 **display ssh server session** 命令查看会话信息，可以看到显示为空，表示之前上线的用户 client001 已下线。

<AC> display ssh server session

| Conn | Ver | Encry | State | Retry | SerType | Username |
|------|-----|-------|-------|-------|---------|----------|
|------|-----|-------|-------|-------|---------|----------|

## 3.5 配置文件

- AC 的配置文件:

#

vlan 100

#

vlan 200

#

vlan 300

```

#
local-user client001
  password cipher $c$3$quTLFMdNMvGbzJHtkzp0LjilmQKSc9SJ5w==
  authorization-attribute level 3
  service-type ssh
#
wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable
#
wlan ap-group default_group
  ap officeap
#
interface Vlan-interface100
  ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface300
  ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 300
  port trunk pvid vlan 100
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
    service-template 1 vlan-id 300
  radio enable
#
ssh server enable
ssh user client001 service-type stelnet authentication-type password
#
user-interface vty 0 4
  authentication-mode scheme
  user privilege level 3
  protocol inbound ssh
#

```

- Switch 的配置文件:

```
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 300
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 100
    poe enable
#
interface GigabitEthernet1/0/3
    port link-type access
    port access vlan 100
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。

# H3C 无线控制器远程 MAC 认证典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                           |    |
|---------------------------|----|
| 1 简介.....                 | 1  |
| 2 配置前提 .....              | 1  |
| 3 配置举例 .....              | 1  |
| 3.1 组网需求 .....            | 1  |
| 3.2 配置注意事项.....           | 1  |
| 3.3 配置步骤.....             | 1  |
| 3.3.1 配置 AC.....          | 1  |
| 3.3.2 配置 Switch.....      | 5  |
| 3.3.3 配置 RADIUS 服务器 ..... | 5  |
| 3.4 验证配置 .....            | 8  |
| 3.5 配置文件 .....            | 8  |
| 4 相关资料 .....              | 10 |



# 1 简介

本文档介绍无线客户端通过 RADIUS 服务器进行 MAC 地址认证的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

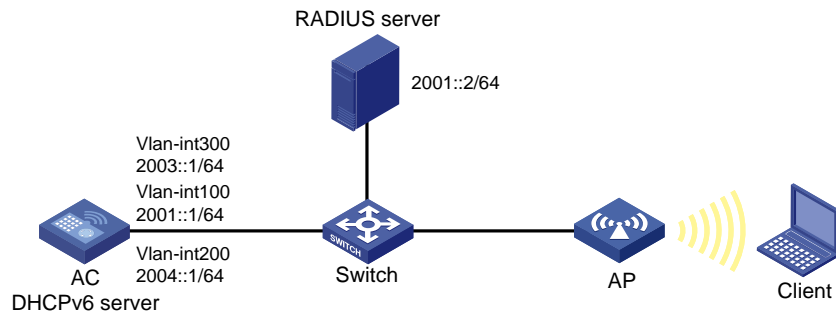
本文档假设您已了解 MAC 地址认证、WLAN 用户接入认证和 WLAN 接入特性。

## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，集中式转发架构下，AP 和 Client 通过 DHCPv6 server 获取 IPv6 地址，要求在 AC 上使用 MAC 地址用户名格式认证方式进行用户身份认证，以控制其对网络资源的访问。

图1 远程 MAC 地址认证配置组网图



### 3.2 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 配置 Switch 和 AP 相连的接口禁止 VLAN 1 报文通过，以防止 AC 上 VLAN 1 内的报文过多。

### 3.3 配置步骤

#### 3.3.1 配置 AC

- (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。AP 将通过该 VLAN 与 AC 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 address 2001::1 64
```

# 取消对 RA 消息发布的抑制。

```
[AC-Vlan-interface100] undo ipv6 nd ra halt
```

# 设置被管理地址配置标志位为 1。

```
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

# 设置其他配置标志位为 1。

```
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，配置 VLAN 300 的接口 IPv6 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ipv6 address 2003::1 64
```

# 取消对 RA 消息发布的抑制。

```
[AC-Vlan-interface300] undo ipv6 nd ra halt
```

# 设置被管理地址配置标志位为 1。

```
[AC-Vlan-interface300] ipv6 nd autoconfig managed-address-flag
```

# 设置其他配置标志位为 1。

```
[AC-Vlan-interface300] ipv6 nd autoconfig other-flag
[AC-Vlan-interface300] quit
```

# 配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置 DHCPv6 server

# 使能 DHCPv6 服务器功能。

```
[AC] ipv6 dhcp server enable
```

# 创建 DHCPv6 地址池 1，配置地址池范围为 2004::/64，为 AP 分配 IPv6 地址。

```
[AC] ipv6 dhcp pool 1
[AC-dhcp6-pool-1] network 2004::/64
[AC-dhcp6-pool-1] quit
```

# 创建 DHCPv6 地址池 2，配置地址池范围为 2003::/64，为 Client 分配 IPv6 地址。

```

[AC] ipv6 dhcp pool 2
[AC-dhcp6-pool-2] network 2003::/64
[AC-dhcp6-pool-2] quit
# 配置 VLAN 接口 100 工作在 DHCPv6 服务器模式，引用地址池 1，为 AP 分配 IPv6 地址。
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 dhcp server apply pool 1
[AC-Vlan-interface100] quit
# 配置 VLAN 接口 300 工作在 DHCPv6 服务器模式，引用地址池 2，为 AP 分配 IPv6 地址。
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ipv6 dhcp server apply pool 2
[AC-Vlan-interface300] quit

```

### (3) 配置 AAA

```

# 创建名字为 office 的 RADIUS 方案并进入该方案视图。
[AC] radius scheme office
# 配置 RADIUS 方案的主认证服务器 IPv6 地址。
[AC-radius-office] primary authentication ipv6 2001::2
# 配置 RADIUS 方案的主计费服务器 IPv6 地址。
[AC-radius-office] primary accounting ipv6 2001::2
# 将 RADIUS 方案 office 的认证报文的共享密钥设置为明文 123456789。
[AC-radius-office] key authentication simple 123456789
# 将 RADIUS 方案 office 的计费报文的共享密钥设置为明文 123456789。
[AC-radius-office] key accounting simple 123456789
# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。
[AC-radius-office] user-name-format without-domain
# 设置设备发送 RADIUS 报文使用的源 IPv6 地址为 2001::1。
[AC-radius-office] nas-ip ipv6 2001::1
[AC-radius-office] quit
# 创建 office 域并进入其视图。
[AC] domain office
# 为 MAC 地址认证用户配置认证方案为 RADIUS 方案，方案名为 office。
[AC-isp-office] authentication lan-access radius-scheme office
# 为 MAC 地址认证用户配置授权方案为 RADIUS 方案，方案名为 office。
[AC-isp-office] authorization lan-access radius-scheme office
# 为 MAC 地址认证用户配置计费方案为 RADIUS 方案，方案名为 office。
[AC-isp-office] accounting lan-access radius-scheme office
[AC-isp-office] quit

```

### (4) 配置 MAC 地址认证

```

# 使能端口安全。
[AC] port-security enable
# 创建 WLAN-ESS1 接口，并进入该视图。
[AC] interface wlan-ess 1
# 设置端口的链路类型为 Hybrid。
[AC-WLAN-ESS1] port link-type hybrid

```

```

# 设置端口允许 VLAN 300 的报文不带 VLAN tag 通过。
[AC-WLAN-ESS1] port hybrid vlan 300 untagged
# 设置端口禁止 VLAN 1 的报文通过。
[AC-WLAN-ESS1] undo port hybrid vlan 1
# 指定端口缺省 VLAN 为 VLAN 300。
[AC-WLAN-ESS1] port hybrid pvid vlan 300
# 使能端口的 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
# 配置 MAC 端口安全模式。
[AC-WLAN-ESS1] port-security port-mode mac-and-psk
# 启用密钥协商功能。
[AC-WLAN-ESS1] port-security tx-key-type 1key
# 配置预共享密钥为 12345678。
[AC-WLAN-ESS1] port-security preshared-key pass-phrase 12345678
# 配置 MAC 地址认证用户使用的 ISP 域为 office。
[AC-WLAN-ESS1] mac-authentication domain office
[AC-WLAN-ESS1] quit
# 配置 MAC 地址认证的用户名和密码均为用户的 MAC 地址（该配置为缺省配置）。
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
# 配置 MAC 地址认证用户使用的 ISP 域为 local-mac。
[AC] mac-authentication domain office

(5) 配置无线服务
# 创建型号为 WA2620E-AGN 的 AP 模板名为 officeap，指定其序列号。
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 配置的服务模板 1 与射频 2 关联，设置绑定到射频接口的 VLAN 编号为 VLAN 300。
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
# 创建无线服务模板 1，并进入无线服务模板视图。
[AC] wlan service-template 1 crypto
# 配置 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到无线服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 配置认证方式为开放认证。
[AC-wlan-st-1] authentication-method open-system
# 启用 CCMP 加密套件。
[AC-wlan-st-1] cipher-suite ccmp

```

```
# 配置安全信息元素为 RSN。
[AC-wlan-st-1] security-ie rsn
# 开启无线服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### 3.3.2 配置 Switch

# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 CAPWAP 隧道内的流量，VLAN 200 用于转发 Client 无线报文。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，禁止 VLAN 1 报文通过，允许 VLAN 100 通过，当前 Trunk 口的 PVID 为 100。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 开启 PoE 接口远程供电功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

### 3.3.3 配置 RADIUS 服务器



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.1(E0303P10)、iMC UAM 7.1(E0303P10)，说明 RADIUS server 的基本配置。

---

#### (1) 增加接入设备

登录进入 iMC 管理平台，“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，单击<增加>按钮，进入“增加接入设备”页面，单击<增加 IPv6 设备>按钮，进入“手工增加接入设备”页面。

- 填写起始 IPv6 地址为“2001::1”。
- 单击<确定>按钮完成操作。

- 在“接入配置”区域配置共享密钥为“123456789”，该共享密钥与 AC 上配置 RADIUS 服务器上的密钥一致。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

## (2) 增加接入规则配置

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，单击<增加>按钮，创建一条接入策略。

- 配置接入策略名为“office”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

## (3) 增加服务配置

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，单击<增加>按钮，创建一条服务。

- 配置服务名为“office\_mac”（这里的服名可以任意命名）。
- 缺省接入策略选择“office”。

- 其他采用默认配置。
- 单击<确定>按钮完成配置。

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

|                                         |                                      |               |        |
|-----------------------------------------|--------------------------------------|---------------|--------|
| 服务名 *                                   | office_mac                           | 服务后缀          |        |
| 业务分组 *                                  | 未分组                                  | 缺省接入策略 *      | office |
| 缺省安全策略 *                                | 不使用                                  | 缺省内网外连策略 *    | 不使用    |
| 缺省私有属性下发策略 *                            | 不使用                                  |               |        |
| 缺省单帐号最大绑定终端数 *                          | 0                                    | 缺省单帐号在线数量限制 * | 0      |
| 服务描述                                    |                                      |               |        |
| <input checked="" type="checkbox"/> 可申请 | <input type="checkbox"/> Portal无感知认证 |               |        |

接入场景列表

| 名称          | 接入策略 | 安全策略 | 私有属性下发策略 | 内网外连策略 | 优先级 | 修改 | 删除 |
|-------------|------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |      |          |        |     |    |    |

确定 取消

#### (4) 增加接入用户

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，单击<增加>按钮，增加一个接入用户。

- 单击<增加用户>按钮，输入用户姓名“adm\_office\_mac”和证件号码“adm\_office\_mac”，单击<确定>按钮完成。

用户 > 接入用户 > 增加接入用户

接入用户

接入信息

|                                              |  |    |      |
|----------------------------------------------|--|----|------|
| 用户姓名 *                                       |  | 选择 | 增加用户 |
| 帐号名 *                                        |  |    |      |
| <input type="checkbox"/> 预开户用户               |  |    |      |
| 密码 *                                         |  |    |      |
| <input checked="" type="checkbox"/> 允许用户修改密码 |  |    |      |
| 生效时间                                         |  |    |      |
| 最大闲置时长(分钟)                                   |  |    |      |
| Portal无感知认证最                                 |  |    |      |
| 登录提示信息                                       |  |    |      |

快速认证用户

修改密码

增加用户

基本信息

|        |                |        |                |        |
|--------|----------------|--------|----------------|--------|
| 用户姓名 * | adm_office_mac | 证件号码 * | adm_office_mac | 检查是否可用 |
| 通讯地址   |                | 电话     |                |        |
| 电子邮件   |                | 用户分组 * | 未分组            |        |

确定 取消

服务名 状态 分配IP地址

- 配置帐号名“admin”和密码“123456”。
- 勾选绑定服务名“office\_mac”。
- 单击<确定>按钮完成。

用户 > 接入用户 > 增加接入用户 帮助

---

接入用户

---

接入信息

用户姓名 \*

帐号名 \*

☐ 预开户用户

密码 \*

☒ 允许用户修改密码

生效时间

最大闲置时长(分钟)

Portal无感知认证最大绑定数 \*

登录提示信息

adm\_office\_mac 选择 增加用户

admin

☐ 缺省BYOD用户

.....

☐ 启用用户密码控制策略

1

☐ MAC地址认证用户

密码确认 \*

☐ 主机名用户

.....

☐ 下次登录须修改密码

失效时间

在线数量限制

☐ 快速认证用户

接入服务

## 3.4 验证配置

# 完成以上配置后，无线用户 Client 连接到 WLAN 网络并进行 MAC 地址认证。在 AC 上通过命令 **display wlan client** 可以看见无线用户 Client 从 VLAN 300 上线。

```
[AC] display wlan client
```

```
Total Number of Clients          : 1
```

| MAC address    | Username     | AP name  | RID | IP address | IPv6 address | VLAN |
|----------------|--------------|----------|-----|------------|--------------|------|
| 3ca9-f414-4c20 | 3ca9f4144c20 | officeap | 2   | N/A        | 2003::2      | 300  |

## 3.5 配置文件

- AC:

```
#
port-security enable
#
mac-authentication domain office
#
ipv6 dhcp server enable
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
primary authentication ipv6 2001::0002
primary accounting ipv6 2001::0002
key authentication cipher $c$3$yo3JtYv4nudQQagshEbNynCWjIaLSmo=
key accounting cipher $c$3$HCq14LPxOPjsJ902EQZaQag57yVGK30=
```



```

user-name-format without-domain
nas-ip ipv6 2001::1
#
domain office
authentication lan-access radius-scheme office
authorization lan-access radius-scheme office
accounting lan-access radius-scheme office
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 1
cipher-suite ccmp
security-ie rsn
#
ipv6 dhcp pool 1
network 2004::/64
#
ipv6 dhcp pool 2
network 2003::/64
#
interface Vlan-interface100
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
ipv6 address 2001::1/64
ipv6 dhcp server apply pool 1
#
interface Vlan-interface300
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
ipv6 address 2003::1/64
ipv6 dhcp server apply pool 2
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 300 untagged

```

```

port hybrid pvid vlan 300
mac-vlan enable
port-security port-mode mac-and-psk
port-security tx-key-type 11key
port-security preshared-key pass-phrase cipher $c$3$ss8YJ7d/nVASN5hgTNJjeg0OK+I
EgsVX80RJ
mac-authentication domain office
#
wlan ap officeap model WA2620E-AGN id 2
serial-id 21023529G007C000020
firmware-update disable
radio 1
radio 2
radio enable
#
• Switch:
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port access vlan 100
poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导(R5208P01)》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考(R5208P01)》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导(R5208P01)》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考(R5208P01)》中的“安全命令参考”。

# 基于 AP 的无线终端准入典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                           |    |
|---------------------------|----|
| 1 简介.....                 | 1  |
| 2 配置前提 .....              | 1  |
| 3 配置举例 .....              | 1  |
| 3.1 组网需求 .....            | 1  |
| 3.2 配置思路 .....            | 2  |
| 3.3 配置注意事项 .....          | 2  |
| 3.4 配置步骤 .....            | 2  |
| 3.4.1 AC 的配置 .....        | 2  |
| 3.4.2 Switch 的配置 .....    | 5  |
| 3.4.3 RADIUS 服务器的配置 ..... | 6  |
| 3.5 验证配置 .....            | 11 |
| 3.6 配置文件 .....            | 13 |
| 4 相关资料 .....              | 16 |

# 1 简介

本文档介绍基于 AP 的无线终端准入，即使无线客户端只能从指定的 AP 接入无线网络的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 接入和 User Profile 特性。

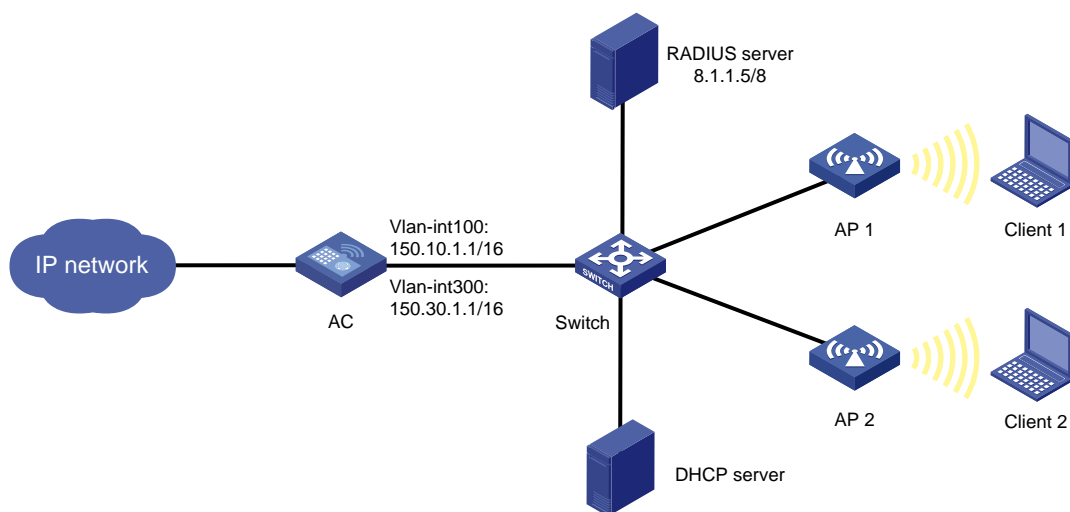
## 3 配置举例

### 3.1 组网需求

如图 1 所示，无线网络中 AC 下关联两台 AP，AP 和 Client 通过 DHCP server 获取 IP 地址。Client 1、Client 2 分别通过 AP 1、AP 2 接入到外部网络。现要求如下：

- AP 1 和 AP 2 划分到 VLAN 100 内，Client 1 和 Client 2 划分到 VLAN 200 内。
- Client 1 只能通过 AP 1 访问网络，而 Client 2 只能通过 AP 2 访问网络。

图1 基于 AP 的用户接入控制组网图



## 3.2 配置思路

- 在 AC 上配置 802.1X 认证，配置主认证服务器的 IP 地址指向 RADIUS server，使 Client 的认证信息能够转发到 RADIUS server 上进行认证。
- 建立 AP 组与 802.1X 用户组，将 AP 管理模板 officeap1 和 officeap2 分别加入到不同的 AP 组中，再将 802.1X 用户组与 AP 组进行绑定。这样就可以确保 Client 只能通过指定的 AP 访问网络资源。

## 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 150.10.1.1 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 150.30.1.1 255.255.0.0
[AC-Vlan-interface300] quit
```

# 配置 AC 的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置认证策略

# 启用端口安全，配置 802.1X 认证方式为 EAP。

```
[AC] port-security enable
```

```

[AC] dot1x authentication-method eap
# 创建 RADIUS 方案 office，将 RADIUS 服务器类型设置为 extended。
[AC] radius scheme office
[AC-radius-office] server-type extended
# 配置 RADIUS 方案的主认证服务器的 IP 地址为 8.1.1.5/8，认证报文的共享密钥设置为明文 123456。
[AC-radius-office] primary authentication 8.1.1.5
[AC-radius-office] key authentication 123456
# 指定发送给 RADIUS 服务器的用户名不得携带 ISP 域名。
[AC-radius-office] user-name-format without-domain
[AC-radius-office] quit
(3) 配置认证域
# 创建名为 office 的 ISP 域，并进入其视图。
[AC] domain office
# 配置 802.1X 用户使用 RADIUS 方案 office 进行认证和授权，不对用户使用的网络服务进行计费。
[AC-isp-office] authentication default radius-scheme office
[AC-isp-office] authorization default radius-scheme office
[AC-isp-office] accounting default none
[AC-isp-office] quit
# 把配置的认证域 office 设置为系统缺省域。
[AC] domain default enable office
(4) 配置无线口的端口安全（802.1X 认证）
# 创建 WLAN ESS 接口 1。
[AC] interface wlan-ess 1
# 配置端口的链路类型为 Hybrid。
[AC-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
# 使能 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
# 配置 WLAN ESS 1 的端口安全模式为 userlogin-secure-ext。
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
# 使能 11key 类型的密钥协商功能。
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 关闭在线用户握手和 802.1X 的组播触发功能。
[AC-WLAN-ESS1] undo dot1x handshake
[AC-WLAN-ESS1] undo dot1x multicast-trigger
[AC-WLAN-ESS1] quit
# 配置到 RADIUS 服务器的静态路由。
[AC] ip route-static 8.1.1.5 255.0.0.0 150.10.1.200
(5) 配置无线服务
# 创建 crypto 类型的服务模板 1。

```

```
[AC] wlan service-template 1 crypto
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS 1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind WLAN-ESS 1
# 使能 TKIP 加密套件。
[AC-wlan-st-1] cipher-suite tkip
# 使能 CCMP 加密套件。
[AC-wlan-st-1] cipher-suite ccmp
# 配置信标和探查帧时携带 RSN IE。
[AC-wlan-st-1] security-ie rsn
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

## (6) 配置 AP

# 创建 AP 1 模板，名称为 officeap1，选择 AP 1 的型号为 WA2620E-AGN，并配置序列号为 21023529G007C000020。

```
[AC] wlan ap officeap1 model WA2620E-AGN
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
# 进入 radio2 射频视图。
[AC-wlan-ap-officeap1] radio 2
# 将服务模板绑定到射频接口。
[AC-wlan-ap-officeap1-radio-2] service-template 1 vlan-id 300
[AC-wlan-ap-officeap1-radio-2] radio enable
```

# 创建 AP 2 模板，名称为 officeap2，选择 AP 2 的型号为 WA2620E-AGN，并配置序列号为 21023529G007C000021。

```
[AC] wlan ap officeap2 model WA2620E-AGN
[AC-wlan-ap-officeap2] serial-id 21023529G007C000021
# 进入 radio2 射频视图。
[AC-wlan-ap-officeap2] radio 2
# 将服务模板绑定到射频接口。
[AC-wlan-ap-officeap2-radio-2] service-template 1 vlan-id 300
[AC-wlan-ap-officeap2-radio-2] radio enable
[AC-wlan-ap-officeap2-radio-2] quit
[AC-wlan-ap-officeap2] quit
```

## (7) 配置 User Profile 和 AP 组

# 配置 AP 组，在 AP 组内添加允许接入的 AP 列表。

```
[AC] wlan ap-group 1
[AC-ap-group1] ap officeap1
[AC-ap-group1] quit
[AC] wlan ap-group 2
[AC-ap-group2] ap officeap2
[AC-ap-group2] quit
```

# 配置基于 802.1X 用户的 user-profile，添加允许接入的 AP 组，并使能 User Profile 功能。



```
[AC] user-profile group1
[AC-user-profile-group1] wlan permit-ap-group 1
[AC-user-profile-group1] quit
[AC] user-profile group1 enable
[AC] user-profile group2
[AC-user-profile-group2] wlan permit-ap-group 2
[AC-user-profile-group2] quit
[AC] user-profile group2 enable
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 和 AC 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过, 并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过, 并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 RADIUS server 相连的 GigabitEthernet1/0/4 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/5 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/5
[Switch-GigabitEthernet1/0/5] port link-type access
[Switch-GigabitEthernet1/0/5] port access vlan 100
[Switch-GigabitEthernet1/0/5] quit
```

### 3.4.3 RADIUS 服务器的配置



说明

下面以 iMC 为例(使用 iMC 版本为: iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)),说明 RADIUS 服务器的基本配置。

# 增加接入设备。

登录进入 iMC 管理平台, 选择“用户”页签, 单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项, 进入“接入设备配置”页面, 在该页面中单击<增加>按钮, 进入“增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”;
- 设置认证及计费的端口号分别为“1812”和“1813”;
- 选择业务类型为“LAN 接入业务”;
- 选择接入设备类型为“H3C”;
- 选择或手工增加接入设备, 添加 IP 地址为 150.10.1.1 的接入设备;
- 其它参数采用缺省值, 并单击<确定>按钮完成操作。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

| 接入配置   |              |          |         |
|--------|--------------|----------|---------|
| 认证端口 * | 1812         | 计费端口 *   | 1813    |
| 组网方式   | 不启用混合组网      | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 接入设备分组   | 无       |
| 共享密钥 * |              | 确认共享密钥 * |         |
| 业务分组   | 未分组          |          |         |

| 设备列表    |            |      |    |    |
|---------|------------|------|----|----|
| 选择      | 手工增加       | 全部清除 |    |    |
| 设备名称    | 设备IP地址     | 设备型号 | 备注 | 删除 |
|         | 150.10.1.1 |      |    |    |
| 共有1条记录。 |            |      |    |    |

确定
取消

# 增加接入策略。

选择“用户”页签, 单击导航树中的[用户/接入策略管理/接入策略管理]菜单项, 进入接入策略管理页面, 在该页面中单击<增加>按钮, 进入“增加接入策略”页面。

- 输入服务名“dot1x auth”;
- 认证证书类型“EAP-PEAP”

- 认证证书子类型 “MS-CHAPV2 认证”
- 下发 User Profile “group1”
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略 ? 帮助

|                                                     |                                                                                                   |                                  |             |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------|-------------|
| <b>基本信息</b> <span style="float: right;">-</span>    |                                                                                                   |                                  |             |
| 接入策略名 *                                             | dot1x auth                                                                                        |                                  |             |
| 业务分组 *                                              | 未分组                                                                                               |                                  |             |
| 描述                                                  |                                                                                                   |                                  |             |
| <b>授权信息</b> <span style="float: right;">-</span>    |                                                                                                   |                                  |             |
| 接入时段                                                | 无 ?                                                                                               | 分配IP地址 *                         | 否           |
| 下行速率(Kbps)                                          |                                                                                                   | 上行速率(Kbps)                       |             |
| 优先级                                                 |                                                                                                   | <input type="checkbox"/> 启用RSA认证 |             |
| 证书认证                                                | <input type="radio"/> 不启用 <input checked="" type="radio"/> EAP证书认证 <input type="radio"/> WAPI证书认证 |                                  |             |
| 认证证书类型                                              | EAP-PEAP认证                                                                                        | 认证证书子类型                          | MS-CHAPV2认证 |
| 下发VLAN                                              |                                                                                                   | 下发用户组                            |             |
| <input checked="" type="checkbox"/> 下发User Profile  | group1                                                                                            |                                  |             |
| <input type="checkbox"/> 下发ACL                      |                                                                                                   |                                  |             |
| <b>认证绑定信息</b> <span style="float: right;">+</span>  |                                                                                                   |                                  |             |
| <b>用户客户端配置</b> <span style="float: right;">+</span> |                                                                                                   |                                  |             |

确定
取消

#### # 增加接入服务。

选择“用户”页签，单击导航树中的[用户/接入策略管理/接入服务管理]菜单项，进入服务列表页面，在该页面中单击<增加>按钮，进入“增加接入服务”页面。

- 输入服务名 “dot1x auth”；
- 缺省接入策略 “dot1x auth”
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 增加接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

基本信息

服务名 \*

dot1x auth

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

dot1x auth

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 (PC

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入“增加用户”页面。增加两个接入用户，账号名分别是 office1\_client、office2\_client，其余配置均相同。下面以增加用户 office1\_client 为例。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户姓名“office”；
- 输入证件号码“12345”；
- 单击“检查是否可用”按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图5 增加用户

增加用户

基本信息

用户姓名 \*

office

证件号码 \*

12345

检查是否可用

通讯地址

电话

电子邮件

用户分组 \*

未分组

确定

取消

- 输入账号名“office1\_client”；
- 输入密码“admin”；
- 在接入服务处选择“dot1x auth”；

- 其他配置保持默认；
- 单击<确定>按钮完成操作。

图6 增加接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

office

选择

增加用户

帐号名 \*

office1\_client

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

.....

密码确认 \*

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                            | 服务后缀 | 状态  | 分配IP地址 |
|------------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> dot1x auth |      | 可申请 |        |
| <input type="checkbox"/> eap-peap              |      | 可申请 |        |
| <input type="checkbox"/> Portal-auth           |      | 可申请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线SSID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

IP地址

MAC地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

## 3.5 验证配置

- (1) Client 通过认证后，可以成功关联 AP，可以通过 **display connection** 命令查看用户连接的相关信息。

```
<AC> display connection
```

```
Index=276 ,Username=office1_client@office
MAC=00-24-01-30-69-1A
IP=N/A
IPv6=N/A
```

```
Index=277 ,Username=office2_client@office
MAC=00-1E-E5-9D-D6-D7
IP=N/A
IPv6=N/A
```

```
Total 2 connection(s) matched.
```

- (2) 根据上面信息显示的索引号，可以通过 **display connection ucibindex** 命令查看用户连接的详细信息。

```
<AC> display connection ucibindex 276
```

```
Index=276 , Username=office1_client@office
MAC=00-24-01-30-69-1A
IP=N/A
IPv6=N/A
```

```
Access=8021X ,AuthMethod=EAP
```

```
Port Type=Wireless-802.11,Port Name=WLAN-DBSS1:3
```

```
Initial VLAN=1, Authorization VLAN=300
```

```
ACL Group=Disable
```

```
User Profile=group1
```

```
CAR=Disable
```

```
Priority=Disable
```

```
Accounting Username=office1_client
```

```
Start=2014-01-09 16:59:36 ,Current=2014-01-09 17:01:30 ,Online=00h01m53s
```

```
Total 1 connection matched.
```

```
<AC> display connection ucibindex 277
```

```
Index=277 , Username=office2_client@office
MAC=00-1E-E5-9D-D6-D7
IP=N/A
IPv6=N/A
```

```
Access=8021X ,AuthMethod=EAP
```

```
Port Type=Wireless-802.11,Port Name=WLAN-DBSS1:2
```

```
Initial VLAN=1, Authorization VLAN=300
```

```
ACL Group=Disable
```

```
User Profile=group2
```

```
CAR=Disable
```

```
Priority=Disable
```

```
Accounting Username=office2_client
```

Start=2014-01-09 16:59:50 ,Current=2014-01-09 17:01:38 ,Online=00h01m49s

Total 1 connection matched.

- (3) 通过 **display wlan client verbose** 命令查看所有无线客户端的详细信息，可以看到用户 **office1\_client** 用户只能通过名为 **officeap1** 的 AP 1 接入无线网络，用户 **office2\_client** 只能通过名为 **officeap2** 的 AP 2 接入无线网络。

<AC> display wlan client verbose

Total Number of Clients : 2

Client Information

```
-----
MAC Address           : 001e-e59d-d6d7
User Name             : office2_client
AID                   : 1
AP Name               : officeap2
Radio Id              : 2
SSID                  : service
BSSID                 : 80f6-2e02-2d30
Port                  : WLAN-DBSS1:2
VLAN                  : 300
State                 : Running
Power Save Mode       : Active
Wireless Mode         : 11gn
Channel Band-width    : 20MHz
SM Power Save Enable  : Disabled
Short GI for 20MHz    : Not Supported
Short GI for 40MHz    : Not Supported
Support MCS Set       : 0,1,2,3,4,5,6,7,8,9,
                       10,11,12,13,14,15
BLOCK ACK-TID 0       : IN
BLOCK ACK-TID 7       : OUT
QoS Mode              : WMM
Listen Interval (Beacon Interval) : 10
RSSI                  : 57
Rx/Tx Rate            : 104/130
Client Type           : RSN
Authentication Method : Open System
Authentication Mode    : Central
AKM Method            : Dot1X
4-Way Handshake State : PTKINITDONE
Group Key State        : IDLE
Encryption Cipher      : CCMP
Roam Status            : Normal
Roam Count             : 0
Up Time (hh:mm:ss)    : 00:03:13
-----
```

Client Information

```
-----
MAC Address           : 0024-0130-691a
```



```

User Name          : officel_client
AID                : 1
AP Name            : officeap1
Radio Id           : 2
SSID               : service
BSSID              : 3822-d61f-1eb0
Port               : WLAN-DBSS1:3
VLAN               : 300
State              : Running
Power Save Mode    : Active
Wireless Mode      : 11gn
Channel Band-width : 20MHz
SM Power Save Enable : Disabled
Short GI for 20MHz : Not Supported
Short GI for 40MHz : Not Supported
Support MCS Set    : 0,1,2,3,4,5,6,7,8,9,
                   10,11,12,13,14,15
BLOCK ACK-TID 0    : BOTH
BLOCK ACK-TID 7    : OUT
QoS Mode           : WMM
Listen Interval (Beacon Interval) : 10
RSSI               : 42
Rx/Tx Rate         : 78/104
Client Type        : RSN
Authentication Method : Open System
Authentication Mode : Central
AKM Method         : Dot1X
4-Way Handshake State : PTKINITDONE
Group Key State     : IDLE
Encryption Cipher   : CCMP
Roam Status         : Normal
Roam Count          : 0
Up Time (hh:mm:ss) : 00:03:26

```

---

## 3.6 配置文件

- AC:

```

#
domain default enable office
#
port-security enable
#
dot1x authentication-method eap
#
vlan 100
#
vlan 200

```

```

#
vlan 300
#
radius scheme office
    server-type extended
    primary authentication 8.1.1.5
    key authentication cipher $c$3$a+bOgUuQpN4m8HdNTtoOTCpAuXumaL6BLNw==
    user-name-format without-domain
#
domain office
    authentication default radius-scheme office
    authorization default radius-scheme office
    accounting default none
    access-limit disable
    state active
    idle-cut disable
    self-service-url disable
#
wlan service-template 1 crypto
    ssid service
    bind WLAN-ESS 1
    cipher-suite tkip
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
wlan ap-group 1
    ap officeap1
#
wlan ap-group 2
    ap officeap2
#
user-profile group1
    wlan permit-ap-group 1
user-profile group2
    wlan permit-ap-group 2
#
interface Vlan-interface100
    ip address 150.10.1.1 255.255.0.0
#
interface Vlan-interface300
    ip address 150.30.1.1 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 300
    port trunk pvid vlan 100
#

```

```

interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
  port-security port-mode userlogin-secure-ext
  port-security tx-key-type 11key
  undo dot1x handshake
  undo dot1x multicast-trigger
#
wlan ap officeap1 model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
    service-template 1 vlan 200
  radio enable
#
wlan ap officeap2 model WA2620E-AGN id 2
  serial-id 21023529G007C000021
  radio 1
  radio 2
    service-template 1 vlan 200
  radio enable
#
ip route-static 8.1.1.5 255.0.0.0 150.10.1.200
#
user-profile group1 enable
user-profile group2 enable
#

```

- **Switch:**

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 300
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access

```

```
port access vlan 100
#
interface GigabitEthernet1/0/4
port link-type access
port access vlan 100
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“三层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“三层技术命令参考”。

# 动态黑名单典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤.....          | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 3 |
| 3.4 验证配置 .....         | 4 |
| 3.5 配置文件 .....         | 6 |
| 4 相关资料 .....           | 7 |

# 1 简介

本文介绍了 AC 使用动态黑名单功能实现对无线客户端进行接入控制的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

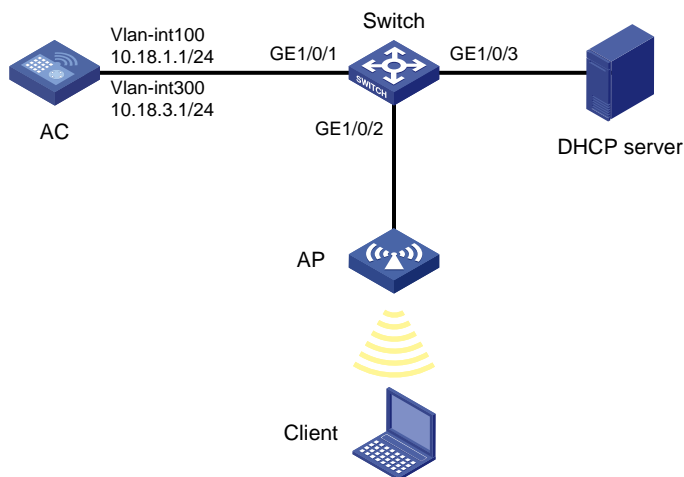
本文档假设您已了解动态黑名单的特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AP 和 Client 通过 DHCP 方式获取 IP 地址。现要求：在 AC 上配置动态黑名单功能，防止 Client 对设备进行泛洪攻击。

图1 动态黑名单配置组网图



### 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.18.1.1 255.255.255.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC-vlan100] quit
[AC] vlan 200
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并配置 VLAN 300 的接口 IP 地址。

```
[AC-vlan200] quit
[AC] vlan 300
[AC-vlan200] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 10.18.3.1 255.255.255.0
[AC-Vlan-interface300] quit
```

# 配置 AC 与 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 模式，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS1 接口，并进入该视图。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置 WLAN-ESS1 接口的缺省 VLAN 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 报文不带 VLAN tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

#### (2) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```



# 设置服务模板 1 的 SSID 为 office。

```
[AC-wlan-st-1] ssid office
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 设置无线客户端接入该无线服务（SSID）的认证方式为开放式系统认证。

```
[AC-wlan-st-1] authentication-method open-system
```

# 开启服务模板 1。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

### (3) 配置射频接口并绑定服务模板

# 创建 AP 管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-officeap] radio 1
```

# 将在 AC 上配置的服务模板 1 映射到射频 1，设置绑定到射频接口的 VLAN 编号为 VLAN 300。

```
[AC-wlan-ap-officeap-radio-1] service-template 1 vlan-id 300
```

```
[AC-wlan-ap-officeap-radio-1] radio enable
```

```
[AC-wlan-ap-officeap-radio-1] quit
```

```
[AC-wlan-ap-officeap] quit
```

### (4) 配置动态黑名单功能

# 在 WLAN IDS 视图下使能攻击检测功能。

```
[AC] wlan ids
```

```
[AC-wlan-ids] attack-detection enable all
```

# 在 WLAN IDS 视图下使能动态黑名单功能。

```
[AC-wlan-ids] dynamic-blacklist enable
```

```
[AC-wlan-ids] quit
```

## 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性 Trunk，禁止 VLAN 1 报文通过，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
```

```
[Switch-GigabitEthernet1/0/3] port link-type access
```

```
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

```
[Switch-GigabitEthernet1/0/3] quit
```

### 3.4 验证配置

# 在 Client 发起泛洪攻击前, Client 可以正常接入无线网络, 通过 **display wlan client verbose** 命令可以观察到该 Client。

```
<AC> display wlan client verbose
```

```
Total Number of Clients : 1
```

```
Client Information
```

```
-----  
MAC Address : 000f-e2cc-ff01
```

```
User Name : -NA-
```

```
AID : 1
```

```
AP Name : ap1
```

```
Radio Id : 1
```

```
SSID : office
```

```
BSSID : 0023-8993-7550
```

```
Port : WLAN-DBSS1:1
```

```
VLAN : 300
```

```
State : Running
```

```
Power Save Mode : Active
```

```
Wireless Mode : 11an
```

```
QoS Mode : WMM
```

```
Listen Interval (Beacon Interval) : 10
```

```
RSSI : 10
```

```
Rx/Tx Rate : 48/36
```

```
Client Type : PRE-RSNA
```

```
Authentication Method : Open System
```

```
AKM Method : None
```

```
4-Way Handshake State : -NA-
```

```
Group Key State : -NA-
```

```
Encryption Cipher : Clear
```

```
Roam Status : Normal
```

Roam Count : 0

Up Time (hh:mm:ss) : 00:09:34

# Client 发起攻击后，AC 上可以检测到泛洪攻击，AC 会将检测到的攻击源加入动态黑名单，在动态黑名单老化期内，AC 会拒绝攻击源的关联请求。此时，可以在 AC 上使用 **display wlan ids statistics** 命令显示检测到的泛洪攻击。

<AC> display wlan ids statistics

Current attack tracking since: 2013-08-29/10:22:07

| Type                                      | Current | Total |
|-------------------------------------------|---------|-------|
| Probe Request Frame Flood Attack          | 0       | 0     |
| Authentication Request Frame Flood Attack | 0       | 0     |
| Deauthentication Frame Flood Attack       | 1       | 1     |
| Association Request Frame Flood Attack    | 0       | 0     |
| Disassociation Request Frame Flood Attack | 0       | 0     |
| Reassociation Request Frame Flood Attack  | 0       | 0     |
| Action Frame Flood Attack                 | 0       | 0     |
| Null Data Frame Flood Attack              | 0       | 0     |
| Weak IVs Detected                         | 0       | 0     |
| Spoofed Deauthentication Frame Attack     | 0       | 0     |
| Spoofed Disassociation Frame Attack       | 0       | 0     |

# 使用 **display wlan blacklist dynamic** 命令显示动态黑名单列表。

<AC> display wlan blacklist dynamic

Total Number of Entries : 1

Dynamic Blacklist

| MAC-Address    | Lifetime(s) | Last Updated Since(hh:mm:ss) | Reason       |
|----------------|-------------|------------------------------|--------------|
| 000f-e2cc-ff01 | 300         | 00:00:04                     | Deauth-Flood |

# Client 停止攻击后，经过黑名单老化时间，使用 **display wlan blacklist dynamic** 命令再次查看黑名单，已经没有信息。

<AC> display wlan blacklist dynamic

Info: Table is empty.

# 使用 **display wlan client verbose** 命令可以观察到无线客户端又重新上线。

<AC> display wlan client verbose

Total Number of Clients : 1

Client Information

|                              |
|------------------------------|
| MAC Address : 000f-e2cc-ff01 |
| User Name : -NA-             |
| AID : 1                      |
| AP Name : ap1                |
| Radio Id : 1                 |
| SSID : office                |
| BSSID : 0023-8993-7550       |

```
Port : WLAN-DBSS1:1
VLAN : 300
State : Running
Power Save Mode : Active
Wireless Mode : 11an
QoS Mode : WMM
Listen Interval (Beacon Interval) : 10
RSSI : 10
Rx/Tx Rate : 48/36
Client Type : PRE-RSNA
Authentication Method : Open System
AKM Method : None
4-Way Handshake State : -NA-
Group Key State : -NA-
Encryption Cipher : Clear
Roam Status : Normal
Roam Count : 0
Up Time (hh:mm:ss) : 00:01:34
```

## 3.5 配置文件

- AC:

```
#
wlan service-template 1 clear
ssid office
bind WLAN-ESS 1
authentication-method open-system
service-template enable
#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
ip address 10.18.1.1 255.255.255.0
#
interface Vlan-interface300
ip address 10.18.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
```

```

undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN
serial-id 21023529G007C000020
radio 1
service-template 1 vlan-id 300
radio enable
#
wlan ids
dynamic-blacklist enable
attack-detection enable all
#

```

#### ● Switch

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 根据上行链路状态控制无线服务典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 2 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 配置 AC .....      | 2 |
| 3.4.2 Switch 的配置 ..... | 4 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 5 |
| 4 相关资料 .....           | 7 |

# 1 简介

本文档介绍根据上行链路状态控制无线服务典型配置举例。

当 AC（Access Controller，无线控制器）的上行链路出现故障，则关闭 AP（Access Point，接入点）射频，禁止无线客户端关联到该 AC 下挂的 AP，以便无线客户端通过上行链路正常工作的 AC 下的 AP 接入网络。如果上行链路恢复正常，则开启 AP 射频，允许无线客户端关联到该 AC 下挂的 AP。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 NQA、Track 和 WLAN 上行链路检测特性。

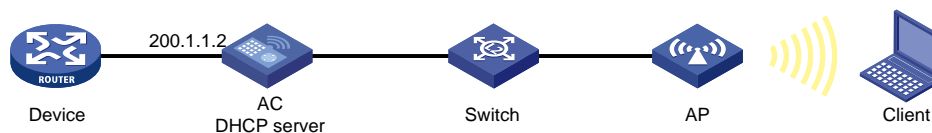
## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 作为局域网用户 Client 访问外部网络的网关，具体要求如下：

- AC 作为 DHCP 服务器，为 AP 和 Client 分配 IP 地址。
- 通过 NQA 监视 AC 的上行链路，当 AC 的上行链路出现故障时，关闭 AP 射频。待 AC 的上行链路故障恢复后，再重新开启 AP 射频。

图1 根据上行链路状态控制无线服务典型配置组网图



### 3.2 配置思路

- 为了使无线网络中的流量便于管理，创建两个 DHCP 地址池，分别为控制流量和业务流量的 VLAN 接口分配 IP 地址。
- 为了实现通过监视 AC 上行链路的状态，从而控制 AC 下挂 AP 射频的开关，需要在 NQA、Track 模块和 WLAN 上行链路检测模块之间建立联动，并采用 NQA 的 ICMP-echo 测试，来判断 AC 与上行设备的链路可达性。



## 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 配置 AC

(1) 配置 AC 的 VLAN 以及 VLAN 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 100.1.1.100 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 200.1.1.200 255.255.0.0
```

# 配置 AC 的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 200 的报文通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN ESS 接口 1。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN ESS 接口的链路类型为 Hybrid，并使能基于 MAC 地址划分 VLAN。

```
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] mac-vlan enable
```

# 配置 VLAN 200 为 Hybrid 端口的缺省 VLAN，禁止通过 VLAN 1 的流量，并且发送 VLAN 200 的报文时不带 VLAN Tag。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] quit
```

(2) 配置 DHCP 服务器

# 在 AC 上开启 DHCP 服务。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 100，为 AP 分配 IP 地址，采用动态绑定方式分配 IP 地址，分配的网段为 100.1.0.0/24，AP 的网关地址为 100.1.1.100

```
[AC] dhcp server ip-pool 100
[AC-dhcp-pool-100] network 100.1.0.0 mask 255.255.255.0
[AC-dhcp-pool-100] gateway-list 100.1.1.100
[AC-dhcp-pool-100] quit
```

# 配置 DHCP 地址池 200，为 Client 分配 IP 地址，采用动态绑定方式分配 IP 地址，分配的网段为 200.1.0.0/24，Client 的网关地址为 200.1.1.200。

```
[AC] dhcp server ip-pool 200
[AC-dhcp-pool-200] network 200.1.0.0 mask 255.255.255.0
[AC-dhcp-pool-200] gateway-list 200.1.1.200
[AC-dhcp-pool-200] quit
```

(3) 配置无线服务。

# 配置 WLAN 服务模板 1，并使用明文方式发送数据。

```
[AC] wlan service-template 1 clear
```

# 配置 SSID 为 service，并将 WLAN-ESS 接口 1 与该服务模板绑定。

```
[AC-wlan-st-1] ssid service
[AC-wlan-st-1] bind wlan-ess 1
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

# 在 AC 上配置 AP 名称为 officeap，型号名称这里选择 WA2620E-AGN，并配置序列号 21023529G007C000020。

```
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio2 视图，将服务模板 1 映射到 radio2，设置 VLAN 200 绑定到 radio2。

```
[AC-wlan-ap-officeap] radio 2
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 200
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

(4) 配置 NQA 测试组。

# 创建 ICMP-echo 类型的 NQA 测试组，并配置测试操作的目的 IP 地址为 200.1.1.2。

```
[AC] nqa entry admin test
[AC-nqa-admin-test] type icmp-echo
[AC-nqa-admin-test-icmp-echo] destination ip 200.1.1.2
```

# 配置连续两次测试开始时间的时间间隔为 1000 毫秒。

```
[AC-nqa-admin-test-icmp-echo] frequency 1000
```

# 配置联动项 1（连续失败 5 次触发联动）。

```
[AC-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type
consecutive 5 action-type trigger-only
[AC-nqa-admin-test-icmp-echo] quit
[AC-nqa-admin-test] quit
```

# 启动 ICMP-echo 测试操作。

```
[AC] nqa schedule admin test start-time now lifetime forever
```

# 配置 Track 项 1，关联 NQA 测试组的联动项 1。

```
[AC] track 1 nqa entry admin test reaction 1
```

# 配置上行链路检测与 Track 项 1 关联。

```
[AC] wlan uplink track 1
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 200 为无线客户端接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 100 通过, 并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

## 3.5 验证配置

在 AC 上通过 **display nqa result** 命令可以查看显示最近一次 NQA 测试的结果。

(1) 在 AC 的上行链路状态正常时, 无线服务正常。

```
[AC] display nqa result
```

```
NQA entry (admin admin, tag test) test results:
```

```
Destination IP address: 200.1.1.2
```

```
Send operation times: 1
```

```
Receive response times: 1
```

```
Min/Max/Average round trip time: 2/2/2
```

```
Square-Sum of round trip time: 4
```

```
Last succeeded probe time: 2014-01-29 10:20:04.3
```

```
Extended results:
```

```
Packet loss in test: 0%
```

```
Failures due to timeout: 0
```

```
Failures due to disconnect: 0
```

```
Failures due to no connection: 0
```

```
Failures due to sequence error: 0
```

```
Failures due to internal error: 0
```

```
Failures due to other errors: 0
```

Packet(s) arrived late: 0

- (2) 用 **shutdown** 命令关闭 AC 连接上行设备的以太网接口，NQA 检测到 AC 与上行设备已断开连接。

[AC] display nqa result

NQA entry (admin admin, tag test) test results:

Destination IP address: 200.1.1.2

Send operation times: 0      Receive response times: 0

Min/Max/Average round trip time: 0/0/0

Square-Sum of round trip time: 0

Last succeeded probe time: 0-00-00 00:00:00.0

Extended results:

Packet loss in test: 100%

Failures due to timeout: 1

Failures due to disconnect: 0

Failures due to no connection: 0

Failures due to sequence error: 0

Failures due to internal error: 0

Failures due to other errors: 0

Packet(s) arrived late: 0

- (3) 用 **undo shutdown** 命令开启 AC 连接上行设备的以太网接口，NQA 检测到 AC 与上行设备重新建立连接。

[AC] display nqa result

NQA entry (admin admin, tag test) test results:

Destination IP address: 200.1.1.2

Send operation times: 1      Receive response times: 1

Min/Max/Average round trip time: 1/1/1

Square-Sum of round trip time: 1

Last succeeded probe time: 2014-01-29 10:33:30.3

Extended results:

Packet loss in test: 0%

Failures due to timeout: 0

Failures due to disconnect: 0

Failures due to no connection: 0

Failures due to sequence error: 0

Failures due to internal error: 0

Failures due to other errors: 0

Packet(s) arrived late: 0

## 3.6 配置文件

- AC:

```
#
port-security enable
#
vlan 100
#
vlan 200
```

```

#
dhcp server ip-pool 100
    network 100.1.0.0 mask 255.255.255.0
    gateway-list 100.1.1.100
#
dhcp server ip-pool 200
    network 200.1.0.0 mask 255.255.255.0
    gateway-list 200.1.1.200
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
interface Vlan-interface100
    ip address 100.1.1.100 255.255.0.0
#
interface Vlan-interface200
    ip address 200.1.1.200 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
nqa entry admin test
    type icmp-echo
    destination ip 200.1.1.2
    frequency 1000
    reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
    trigger-only
#
wlan ap officeap model WA2620E-AGN id 1
    serial-id 21023529G007C000020
    radio 1
    radio 2
    service-template 1 vlan-id 200
    radio enable
#
track 1 nqa entry admin test reaction 1
#

```

```

dhcp enable
#
nqa schedule admin test start-time now lifetime forever
#
wlan uplink track 1
#
•   Switch:
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“网络管理和监控配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“网络管理和监控命令参考”。

# 基于 AP 划分无线终端接入 VLAN 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 1 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 4 |
| 3.5 验证配置 .....         | 5 |
| 3.6 配置文件 .....         | 6 |
| 4 相关资料 .....           | 8 |



# 1 简介

本文档介绍了基于 AP 为接入的无线客户端划分 VLAN 的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

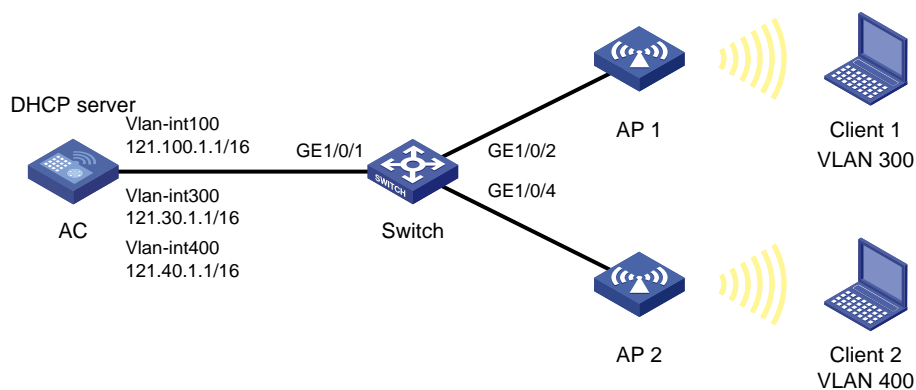
本文档假设您已了解 WLAN 接入的相关特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 通过 Switch 连接 AP，AC 当 DHCP 服务器分别为 Client 和 AP 分配 IP 地址。现要求配置基于 AP 为无线客户端划分 VLAN，具体实现：通过 AP 1 接入的 Client 划分到 VLAN 300，通过 AP 2 接入的 Client 划分到 VLAN 400。

图1 基于 AP 为接入的无线客户端划分 VLAN 配置组网图



### 3.2 配置思路

为了实现基于 AP 为接入的 Client 划分 VLAN，需要配置不同的地址池分别为经 AP 1 和 AP 2 接入的 Client 分配 IP 地址，并在 AC 上配置相应的网关地址。

### 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 121.100.1.1 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 1 接入的业务 VLAN，配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 121.30.1.1 16
[AC-Vlan-interface300] quit
```

# 创建 VLAN 400 作为 Client 2 接入的业务 VLAN，配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 400
[AC-vlan400] quit
[AC] interface vlan-interface 400
[AC-Vlan-interface400] ip address 121.40.1.1 16
[AC-Vlan-interface400] quit
```

# 配置 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100、VLAN 300 和 VLAN 400 通过，设置 PVID 为 VLAN 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300 400
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 DHCP 服务

# 使能 DHCP 服务。

```
[AC] dhcp enable
```

# 创建名为 vlan100 的 DHCP 地址池，为 AP 分配网段为 121.100.0.0/16，网关地址为 121.100.1.1。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 121.100.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan100] gateway-list 121.100.1.1
[AC-dhcp-pool-vlan100] quit
```

# 创建名为 **vlan300** 的 DHCP 地址池，为接入 **AP 1** 的 Client 分配网段为 **121.30.0.0/16**，网关地址为 **121.30.1.1**。

```
[AC] dhcp server ip-pool vlan300
[AC-dhcp-pool-vlan300] network 121.30.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan300] gateway-list 121.30.1.1
[AC-dhcp-pool-vlan300] quit
```

# 创建名为 **vlan400** 的 DHCP 地址池，为接入 **AP 2** 的 Client 分配网段为 **121.40.0.0/16**，网关地址为 **121.40.1.1**。

```
[AC] dhcp server ip-pool vlan400
[AC-dhcp-pool-vlan400] network 121.40.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan400] gateway-list 121.40.1.1
[AC-dhcp-pool-vlan400] quit
```

### (3) 配置 WLAN-ESS 接口

# 创建 **WLAN-ESS1** 接口，并设置端口的链路类型为 **Hybrid** 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 **Hybrid** 端口的 **PVID** 为 **VLAN 200**，禁止 **VLAN 1** 通过并允许 **VLAN 200** 不带 **tag** 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 **MAC VLAN** 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

# 创建 **WLAN-ESS2** 接口，并设置端口的链路类型为 **Hybrid** 类型。

```
[AC] interface wlan-ess 2
[AC-WLAN-ESS2] port link-type hybrid
```

# 配置当前 **Hybrid** 端口的 **PVID** 为 **200**，禁止 **VLAN 1** 通过并允许 **VLAN 200** 不带 **tag** 通过。

```
[AC-WLAN-ESS2] undo port hybrid vlan 1
[AC-WLAN-ESS2] port hybrid vlan 200 untagged
[AC-WLAN-ESS2] port hybrid pvid vlan 200
```

# 使能 **MAC VLAN** 功能。

```
[AC-WLAN-ESS2] mac-vlan enable
[AC-WLAN-ESS2] quit
```

### (4) 配置无线服务模板

# 创建 **clear** 类型的服务模板 **1**。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 **SSID** 为 **service1**。

```
[AC-wlan-st-1] ssid service1
```

# 将 **WLAN-ESS1** 接口绑定到服务模板 **1**。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

# 创建 **clear** 类型的服务模板 **2**。

```

[AC] wlan service-template 2 clear
# 设置当前服务模板的 SSID 为 service2。
[AC-wlan-st-2] ssid service2
# 将 WLAN-ESS2 接口绑定到服务模板 2。
[AC-wlan-st-2] bind wlan-ess 2
# 启用无线服务。
[AC-wlan-st-2] service-template enable
[AC-wlan-st-2] quit
(5) 配置射频接口并绑定服务模板
# 创建 AP 1 的管理模板, 名称为 officeap1, 型号选择 WA2620E-AGN。
[AC] wlan ap officeap1 model WA2620E-AGN
# 设置 AP 1 的序列号为 210235A29G007C000020。
[AC-wlan-ap-officeap1] serial-id 210235A29G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap1] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联, 设置绑定到射频接口的 VLAN 编号为 VLAN 300。
[AC-wlan-ap-officeap1-radio-2] service-template 1 vlan-id 300
# 使能 AP 1 的 radio 2。
[AC-wlan-ap-officeap1-radio-2] radio enable
[AC-wlan-ap-officeap1-radio-2] quit
# 创建 AP 2 的管理模板, 名称为 officeap2, 型号选择 WA2620E-AGN。
[AC] wlan ap officeap2 model WA2620E-AGN
# 设置 AP 2 的序列号为 210235A29G007C000021。
[AC-wlan-ap-officeap2] serial-id 210235A29G007C000021
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap2] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 2 与射频 2 进行关联, 设置绑定到射频接口的 VLAN 编号为 VLAN 400。
[AC-wlan-ap-officeap2-radio-2] service-template 2 vlan-id 400
# 使能 AP 2 的 radio 2。
[AC-wlan-ap-officeap2-radio-2] radio enable
[AC-wlan-ap-officeap2-radio-2] quit
[AC-wlan-ap-officeap2] quit
(6) 使能 ARP Snooping 功能
# 在全局视图下使能 ARP Snooping 功能。
[AC] arp-snooping enable

```

### 3.4.2 Switch 的配置

```

# 创建 VLAN 100、VLAN 300 和 VLAN 400, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 和 VLAN 400 为无线客户端接入的 VLAN。
<Switch> system-view
[Switch] vlan 100

```

```
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] vlan 400
[Switch-vlan400] quit
```

# 配置 Switch 与 AC 连接的 GigabitEthernet1/0/1 接口属性 Trunk，禁止 VLAN 1 报文通过，配置 PVID 为 100，允许 VLAN 100、VLAN 300 和 VLAN 400 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300 400
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/4 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/4 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
```

## 3.5 验证配置

# 使用命令 **display wlan client** 显示所有无线客户端的信息。

```
<AC> display wlan client
```

```
Total Number of Clients          : 2
                                Client Information
```

```
SSID: service1
```

```
-----
MAC Address      User Name      APID/RID IP Address      VLAN
-----
0024-0130-694e -NA-          1 / 2   121.30.0.10      300
-----
```

```
SSID: service2
```

```
-----
MAC Address      User Name      APID/RID IP Address      VLAN
-----
0040-96b3-8a77 -NA-          2 / 2   121.40.0.10      400
-----
```

可以看到，Client 1 连接无线服务 service1，通过 officeap1 接入网络，获取到 VLAN 300 的地址。  
Client 2 连接无线服务 service2，通过 officeap2 接入网络，获取到 VLAN 400 的地址。

## 3.6 配置文件

- AC:

```
#
dhcp server ip-pool vlan100
    network 121.100.0.0 mask 255.255.0.0
    gateway-list 121.100.1.1
#
dhcp server ip-pool vlan300
    network 121.30.0.0 mask 255.255.0.0
    gateway-list 121.30.1.1
#
dhcp server ip-pool vlan400
    network 121.40.0.0 mask 255.255.0.0
    gateway-list 121.40.1.1
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
wlan service-template 1 clear
    ssid service1
    bind WLAN-ESS 1
service-template enable
#
wlan service-template 2 clear
    ssid service2
    bind WLAN-ESS 2
    service-template enable
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 300 400
    undo port trunk permit vlan 1
    port trunk pvid vlan 100
#
interface Vlan-interface100
    ip address 121.100.1.1 255.255.0.0
#
interface Vlan-interface300
    ip address 121.30.1.1 255.255.0.0
```

```

#
interface Vlan-interface400
 ip address 121.40.1.1 255.255.0.0
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
#
interface WLAN-ESS2
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
#
wlan ap officeap1 model WA2620E-AGN id 1
serial-id 210235A29G007C000020
 radio 1
 radio 2
 service-template 1 vlan-id 300
 radio enable
#
wlan ap officeap2 model WA2620E-AGN id 2
serial-id 210235A29G007C000021
 radio 1
 radio 2
 service-template 2 vlan-id 400
 radio enable
#
 arp-snooping enable
#
 dhcp enable
#
● Switch:
#
vlan 100
#
vlan 300
#
vlan 400
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 300 400
 undo port trunk permit vlan 1

```

```
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/4
port link-type access
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。



# 基于 SSID 的 Web 界面访问控制典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 1 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 4 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 6 |
| 4 相关资料 .....           | 7 |

# 1 简介

本文档介绍基于 SSID 的 Web 界面访问控制的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 接入，WLAN ACL 和 HTTP 特性。

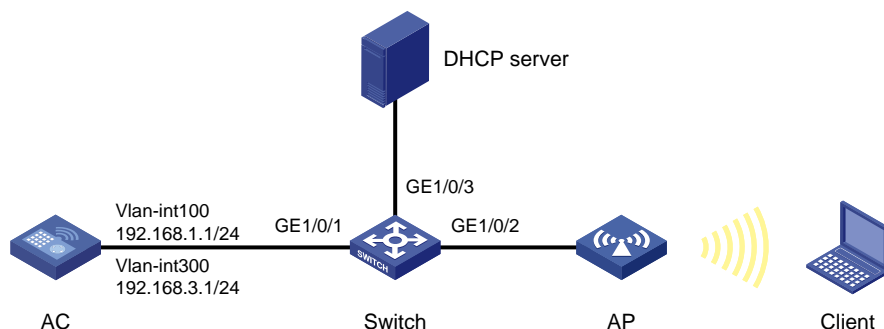
## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 通过 Switch 与 AP 相连，DHCP 服务器为 AP 和 Client 分配 IP 地址。需要控制不同 SSID 接入的无线客户端通过 Web 页面对 AC 的访问权限，具体实现如下：

- 当 Client 通过名为“service2”的 SSID 接入无线网络时，可以通过 Web 访问 AC。
- 而当 Client 通过名为“service1”的 SSID 接入时，不能通过 Web 访问 AC。

图1 基于 SSID 的 Web 界面访问控制组网图



### 3.2 配置思路

为了使关联 SSID 为 service2 的 Client 能够通过 Web 访问 AC，需要在 AC 上配置 WLAN ACL，仅允许关联 SSID 为 service2 的 Client 报文通过，并将 HTTP 服务与 WLAN ACL 相关联。

### 3.3 配置注意事项

- WLAN ACL 中有默认规则 **rule 0 deny**，需要执行 **undo rule 0** 命令删除该默认规则。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.1 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 192.168.3.1 24
[AC-Vlan-interface300] quit
```

# 配置 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，配置 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

# 创建 WLAN-ESS2 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 2
[AC-WLAN-ESS2] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS2] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS2] port hybrid vlan 200 untagged
[AC-WLAN-ESS2] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS2] mac-vlan enable
[AC-WLAN-ESS2] quit
```

## (2) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service1。

```
[AC-wlan-st-1] ssid service1
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

# 创建 clear 类型的服务模板 2。

```
[AC] wlan service-template 2 clear
```

# 设置当前服务模板的 SSID 为 service2。

```
[AC-wlan-st-2] ssid service2
```

# 将 WLAN-ESS2 接口绑定到服务模板 2。

```
[AC-wlan-st-2] bind wlan-ess 2
```

# 启用无线服务。

```
[AC-wlan-st-2] service-template enable
[AC-wlan-st-2] quit
```

## (3) 配置射频接口并绑定服务模板

# 创建 AP 的管理模板，名称为 officeap，型号选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 210235A29G007C000020。

```
[AC-wlan-ap-officeap] serial-id 210235A29G007C000020
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 1 和服务模板 2 与射频 2 进行关联，设置绑定到射频接口的 VLAN 编号为 VLAN 300。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

```
[AC-wlan-ap-officeap-radio-2] service-template 2 vlan-id 300
```

# 使能 AP 的 radio 2。

```
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
```

## (4) 配置 WLAN ACL

# 创建 WLAN ACL 199，并删除 ACL 199 中的默认规则 0。

```
[AC] acl number 199
```

```
[AC-acl-wlan-199] undo rule 0
```

# 配置规则 1：允许 SSID 名称为 service2 的 WLAN 用户报文通过。

```
[AC-acl-wlan-199] rule 1 permit ssid service2
[AC-acl-wlan-199] quit
# 将 HTTP 服务与 ACL 199 关联。
[AC] ip http acl 199
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 的 GigabitEthernet1/0/1 接口属性 Trunk, 禁止 VLAN 1 报文通过, 允许 VLAN 100 和 VLAN 300 通过, 配置 PVID 为 100。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

## 3.5 验证配置

# 无线客户端关联 SSID service2 后, 可以通过 Web 正常访问 AC。



# 无线客户端关联 SSID service1 后，无法通过 Web 访问 AC。



## 3.6 配置文件

- AC:

```
#
ip http acl 199
#
acl number 199
rule 1 permit ssid service2
#
vlan 100
#
vlan 200
#
vlan 300
#
wlan service-template 1 clear
ssid service1
bind WLAN-ESS 1
service-template enable
#
wlan service-template 2 clear
ssid service2
bind WLAN-ESS 2
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
undo port trunk permit vlan 1
port trunk pvid vlan 100
#
interface Vlan-interface100
ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface300
ip address 192.168.3.1 255.255.255.0
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
interface WLAN-ESS2
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
```



```

port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
serial-id 210235A29G007C000020
radio 1
radio 2
service-template 1 vlan-id 300
service-template 2 vlan-id 300
radio enable
#

```

- **Switch:**

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
undo port trunk permit vlan 1
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“基础配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“基础命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“ACL 和 QoS 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“ACL 和 QoS 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 基于 SSID 和基于 VLAN 的用户隔离典型配置 举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                          |    |
|--------------------------|----|
| 1 简介.....                | 1  |
| 2 配置前提 .....             | 1  |
| 3 基于 VLAN 的用户隔离配置举例..... | 1  |
| 3.1 组网需求 .....           | 1  |
| 3.2 配置注意事项.....          | 1  |
| 3.3 配置步骤 .....           | 2  |
| 3.3.1 AC 的配置 .....       | 2  |
| 3.3.2 Switch 的配置 .....   | 3  |
| 3.4 验证配置 .....           | 4  |
| 3.5 配置文件 .....           | 4  |
| 4 基于 SSID 的用户隔离配置举例..... | 6  |
| 4.1 组网需求 .....           | 6  |
| 4.2 配置注意事项.....          | 6  |
| 4.3 配置步骤 .....           | 6  |
| 4.3.1 AC 的配置 .....       | 6  |
| 4.3.2 Switch 的配置 .....   | 8  |
| 4.4 验证配置 .....           | 8  |
| 4.5 配置文件 .....           | 9  |
| 5 相关资料 .....             | 10 |

# 1 简介

本文介绍了基于 VLAN 和基于 SSID 的用户隔离典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解用户隔离特性。

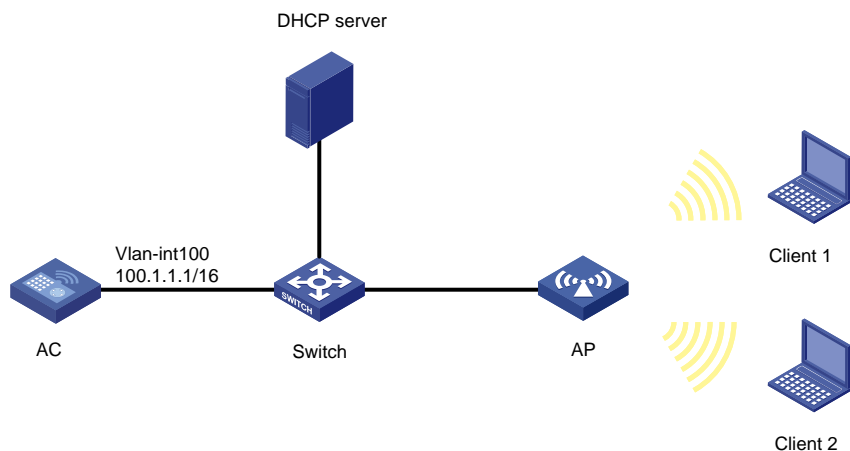
## 3 基于 VLAN 的用户隔离配置举例

### 3.1 组网需求

如[图 1](#)所示，DHCP 服务器为 AP 和 Client 分配 IP 地址，Client 通过 AP 接入无线网络。由于处于同一 VLAN 的用户是能够互访的，这可能带来安全性问题，采用基于 VLAN 的用户隔离，解决此问题，具体要求如下：

- AP 和 Client 正常上线；
- 同一 VLAN 的两台 Client 无法互访。

图1 基于 VLAN 的用户隔离配置组网图



### 3.2 配置注意事项

- 为了使用户隔离不会影响用户与网关的互通，将网关地址加入用户隔离允许列表。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 100.1.1.1 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，配置 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 和 VLAN 300 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 WLAN-ESS 口和服务模板

# 创建编号为 1 的 WLAN-ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

# 创建 clear 类型的无线服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 使能服务模板。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### (3) 配置 AP 模板

# 创建一个 AP 管理模板，其名称为 **officeap**，型号名称为 **WA2620E-AGN**。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
[AC-wlan-ap-officeap] radio 2
```

# 设置绑定到射频接口的 VLAN 编号为 300。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

### (4) 将网关的 MAC 地址加入到启用用户隔离的 VLAN 允许通过的 MAC 地址列表中

```
[AC] user-isolation vlan 300 permit-mac 5866-ba84-8e68
```

### (5) 配置基于 VLAN 的隔离功能

```
[AC] user-isolation vlan 300 enable
```

### (6) 开启 ARP Snooping 功能使 AC 上可以显示学习到的 Client 的 IP 地址

```
[AC] arp-snooping enable
```

## 3.3.2 Switch 的配置

# 创建 VLAN 100，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 用于无线用户的接入。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止 VLAN 1 通过，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

## 3.4 验证配置

(1) 使能基于 VLAN 的用户隔离前，同一 VLAN 内的两台 Client 之间可以互通

# 通过命令 **display wlan client** 查看在线的 Client，可以看到两个 Client 都在 VLAN 300 内。

```
[AC] display wlan client
```

```
Total Number of Clients          : 2
```

```
Client Information
```

```
SSID: service
```

```
-----
MAC Address      User Name      APID/RID IP Address      VLAN
-----
001e-583f-0895 -NA-          1 /2   30.1.0.1         300
2477-0341-f118 -NA-          1 /2   30.1.0.2         300
-----
```

# Client 1 与 Client 2 之间可以互通，此时在 VLAN 300 内无线客户端可以互相访问。

```
C:\Windows\System32>ping 30.1.0.2
```

```
Pinging 30.1.0.2 with 32 bytes of data:
```

```
Reply from 30.1.0.2: bytes=32 time=1ms TTL=128
```

```
Reply from 30.1.0.2: bytes=32 time=25ms TTL=128
```

```
Reply from 30.1.0.2: bytes=32 time<1ms TTL=128
```

```
Reply from 30.1.0.2: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 30.1.0.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 25ms, Average = 6ms
```

(2) 使能基于 VLAN 的用户隔离后，两台 Client 无法互通。

# Client 1 无法 ping 通 Client 2，此时在 VLAN 300 内无线客户端无法互相访问。

```
C:\Windows\System32>ping 30.1.0.2
```

```
Pinging 30.1.0.2 with 32 bytes of data:
```

```
Reply from 192.168.100.24: Destination host unreachable.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 30.1.0.2:
```

```
Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
```

## 3.5 配置文件

```
#
user-isolation vlan 300 enable
user-isolation vlan 300 permit-mac 5866-ba84-8e68
#
vlan 100
```

```

#
vlan 200
#
vlan 300
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk pvid vlan 100
    port trunk permit vlan 100 300
#
interface Vlan-interface100
    ip address 100.1.1.1 255.255.0.0
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
wlan ap office model WA2620E-AGN id 1
    serial-id 21023529G007C000020
    radio 1
    radio 2
        service-template 1 vlan-id 300
    radio enable
#
arp-snooping enable
#

```

## - Switch

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 300
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2

```



```
port link-type access
port access vlan 100
poe enable
#
```

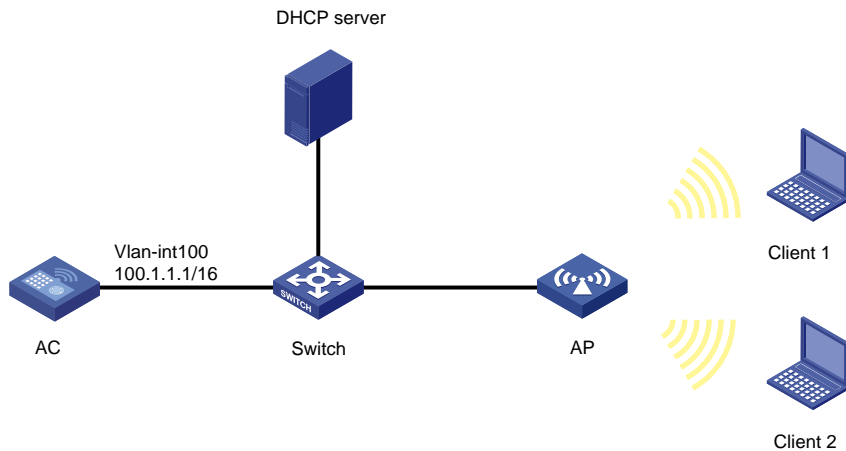
## 4 基于 SSID 的用户隔离配置举例

### 4.1 组网需求

如图 2 所示，DHCP 服务器为 AP 和 Client 分配 IP 地址，Client 通过 AP 接入无线网络。由于处于同一 SSID 的用户是能够互访的，这可能带来安全性问题，采用基于 SSID 的用户隔离，解决此问题，具体要求如下：

- AP 和 Client 正常上线；
- 接入同一 SSID 的两台 Client 无法互访。

图2 基于 SSID 的用户隔离配置组网图



### 4.2 配置注意事项

- 基于 SSID 的用户隔离只能在服务模板未使能的情况下开启或关闭。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 4.3 配置步骤

#### 4.3.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
```

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 100.1.1.1 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，配置 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 和 VLAN 300 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置 WLAN-ESS 口和服务模板

# 创建编号为 1 的 WLAN-ESS 接口，配置端口的链路类型为 Hybrid，并禁止 VLAN1 通过当前的 Hybrid 端口。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

# 创建 clear 类型的无线服务模板 1。

```
[AC] wlan service-template 1 clear
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
[AC-wlan-st-1] quit
```

## (3) 配置 AP 模板

# 创建一个 AP 管理模板，其名称为 officeap，型号名称为 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 AP 的 radio 2 射频视图，配置服务模板与射频 2 进行关联。

```
[AC-wlan-ap-officeap] radio 2
[AC-wlan-ap-officeap] radio 2
```

# 设置绑定到射频接口的 VLAN 编号为 300。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

# 使能 AP 的 radio 2 射频。

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

```
[AC-wlan-ap-officeap] quit
```

(4) 配置基于 SSID 的隔离功能，使能服务模板

```
[AC] wlan service-template 1
```

```
[AC-wlan-st-1] user-isolation enable
```

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

(5) 使能 ARP Snooping 功能，使 AC 可以显示学习到的 IP 地址

```
[AC] arp-snooping enable
```

### 4.3.2 Switch 的配置

# 创建 VLAN 100，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 用于无线用户的接入。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

## 4.4 验证配置

(1) 使能基于 SSID 的用户隔离前，接入同一 SSID 的两台 Client 之间可以互访

# 通过命令 **display wlan client** 查看在线的 Client，两台 Client 接入同一 SSID。

```
[AC] display wlan client
```

```
Total Number of Clients          : 2
```

```
Client Information
```

```
SSID: service
```

| MAC Address         | User Name | APID/RID | IP Address | VLAN |
|---------------------|-----------|----------|------------|------|
| 001e-583f-0895 -NA- |           | 1 /2     | 30.1.0.1   | 300  |
| 2477-0341-f118 -NA- |           | 1 /2     | 30.1.0.2   | 300  |

# Client 1 与 Client 2 之间可以互通，接入同一 SSID 的两台 Client 之间可以互访。

```
C:\Windows\System32>ping 30.1.0.2
```

```
Pinging 30.1.0.2 with 32 bytes of data:
Reply from 30.1.0.2: bytes=32 time=1ms TTL=128
Reply from 30.1.0.2: bytes=32 time=25ms TTL=128
Reply from 30.1.0.2: bytes=32 time<1ms TTL=128
Reply from 30.1.0.2: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 30.1.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 25ms, Average = 6ms
```

(2) 使能用户隔离后，接入同一 SSID 的两台 Client 无法互访

# Client 1 无法 ping 通 Client 2，接入同一 SSID 的两台 Client 之间无法互访。

```
C:\Windows\System32>ping 30.1.0.2
```

```
Pinging 30.1.0.2 with 32 bytes of data:
Reply from 192.168.100.24: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 30.1.0.2:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
```

## 4.5 配置文件

```

• AC
#
vlan 100
#
vlan 200
#
Vlan 300
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
user-isolation enable
service-template enable

```

```

#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk pvid vlan 100
port trunk permit vlan 100 300
#
interface Vlan-interface100
ip address 100.1.1.1 255.255.0.0
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1 vlan-id 300
radio enable
#
arp-snooping enable
#
•   Switch
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#

```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。

- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 基于 VLAN 池授权 VLAN 应用典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |    |
|------------------------|----|
| 1 简介.....              | 1  |
| 2 配置前提 .....           | 1  |
| 3 配置举例 .....           | 1  |
| 3.1 组网需求 .....         | 1  |
| 3.2 配置思路 .....         | 2  |
| 3.3 配置注意事项.....        | 2  |
| 3.4 配置步骤 .....         | 2  |
| 3.4.1 AC 的配置 .....     | 2  |
| 3.4.2 Switch 的配置 ..... | 4  |
| 3.5 验证配置 .....         | 5  |
| 3.6 配置文件 .....         | 8  |
| 4 相关资料 .....           | 10 |



# 1 简介

本文介绍了基于 VLAN 池授权 VLAN 应用的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 VLAN 池的特性。

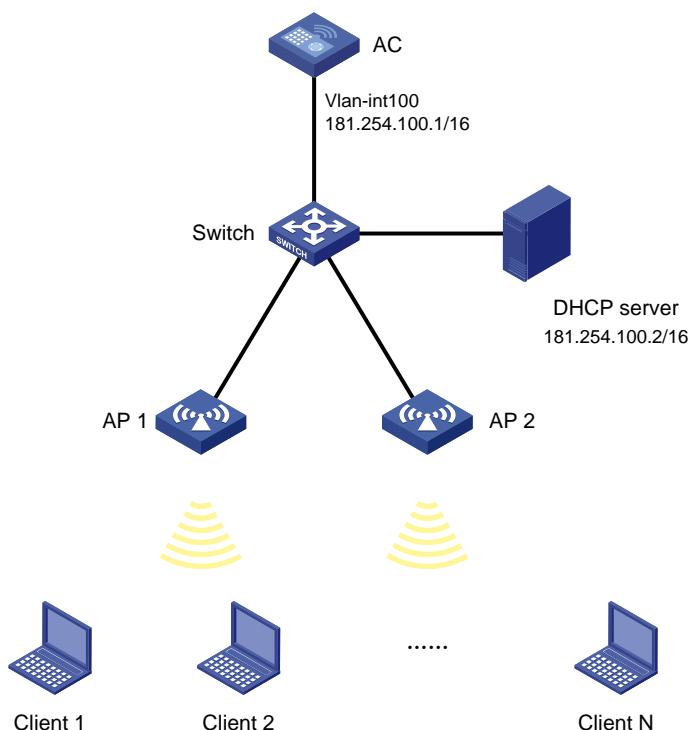
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，AC 通过 Switch 与 AP 1、AP 2、DHCP 服务器相连，DHCP 服务器分别为 AP 和 Client 分配 IP 地址。为了避免过多的 Client 集中在同一 VLAN 内，缓解单 VLAN 内的网络压力。现要求：

- 配置 VLAN 1000~VLAN 1010 作为 Client 接入的 VLAN，并加入到 VLAN 地址池中。
- 当多个 Client 先后上线时，AC 将从 VLAN 池中按由小到大的顺序依次为 Client 下发 VLAN，DHCP 服务器从对应的 VLAN 地址池为 Client 分配地址，确保 Client 能够均匀的分布在上述 VLAN 中。

图1 基于 VLAN 池应用的无线接入控制组网图



## 3.2 配置思路

为了实现无线客户端能够均匀分布在不同 VLAN 中，需要将 VLAN 池绑定到对应的无线服务上。

## 3.3 配置注意事项

- VLAN 池将 VLAN ID 分配给无线客户端后，如果该无线客户端下线，并在一定时间内（默认为 3 分钟）再次通过同一 SSID 上线，那么 VLAN 池不会再次给该无线客户端分配 VLAN，无线客户端会直接继承上次 VLAN 池分配的 VLAN，使用 **display wlan statistics client vlan-pool** 命令统计 VLAN 池中各 VLAN 中的无线客户端数量时，也不会将该无线客户端统计在内。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

(1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
```

```
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 181.254.100.1 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 1000~VLAN 1010 作为 Client 接入的业务 VLAN。

```
[AC] vlan 1000 to 1010
```

# 配置接口 VLAN 1000~VLAN 1010 的 IP 地址。

```
[AC] interface vlan-interface 1000
[AC-Vlan-interface1000] ip address 181.254.0.1 24
[AC-Vlan-interface1000] quit
[AC] interface vlan-interface 1001
[AC-Vlan-interface1001] ip address 181.254.1.1 24
[AC-Vlan-interface1001] quit
```

VLAN 1002~VLAN 1010 的 IP 地址依次递增，配置方法同上。

# 配置 AC 与 Switch 相连的 GigabitEthernet 1/0/1 接口为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100、VLAN 1000~VLAN 1010 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 1000 to 1010
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS1 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS 1 接口类型为 Hybrid 类型。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置 Hybrid 端口 PVID 为 VLAN 200，禁止 VLAN 1 报文通过并允许 VLAN 200 报文不带 VLAN tag 通过。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

## (2) 配置 VLAN 池

# 创建一个名为 vp1 的 VLAN 池，配置 VLAN 池中的 VLAN 列表为 VLAN 1000~VLAN 1010。

```
[AC] wlan vlan-pool vp1
[AC-wlan-vp-vp1] vlan-id 1000 to 1010
[AC-wlan-vp-vp1] quit
```

## (3) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID（服务模板的标识）为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 使能无线模板。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

#### (4) 配置 AP

# 创建 AP 1 的管理模板，其名称为 officeap1，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap1 model WA2620E-AGN
```

# 设置 AP 1 的序列号为 210235A29G007C000020。

```
[AC-wlan-ap-officeap1] serial-id 210235A29G007C000020
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-officeap1] radio 1
```

# 将在 AC 上配置的服务模板 1 与射频 1 进行关联，设置绑定到射频接口的 VLAN 池为 vp1。

```
[AC-wlan-ap-officeap1-radio-1] service-template 1 vlan-pool vp1
```

# 使能 AP 1 的 radio 1。

```
[AC-wlan-ap-officeap1-radio-1] radio enable
```

```
[AC-wlan-ap-officeap1-radio-1] quit
```

```
[AC-wlan-ap-officeap1] quit
```

# 创建 AP 2 的管理模板，其名称为 officeap2，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap2 model WA2620E-AGN
```

# 设置 AP 2 的序列号为 210235A29G007C000021。

```
[AC-wlan-ap-officeap2] serial-id 210235A29G007C000021
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-officeap2] radio 1
```

# 将在 AC 上配置的服务模板 1 与射频 1 进行关联，设置绑定到射频接口的 VLAN 池为 vp1。

```
[AC-wlan-ap-officeap2-radio-1] service-template 1 vlan-pool vp1
```

# 使能 AP 2 的 radio 1。

```
[AC-wlan-ap-officeap2-radio-1] radio enable
```

```
[AC-wlan-ap-officeap2-radio-1] quit
```

```
[AC-wlan-ap-officeap2] quit
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 1000~VLAN 1010，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 1000~VLAN 1010 为无线客户端接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 1000 to 1010
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk，禁止 VLAN 1 报文通过，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 1000~VLAN 1010 通过。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 1000 to 1010
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/4 接口属性为 Access，并允许 VLAN 100 通过。
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

### 3.5 验证配置

当有大量的无线客户端通过 **SSID service** 上线，查看无线客户端上线情况。

# 使用命令 **display wlan client** 查看是否有无线客户端在线，无线客户端通过同一个服务模板不同的 AP 上线（篇幅有限，只显示一部分用户）。

```
<AC> display wlan client
Total Number of Clients          : 128
                                Client Information
SSID: service
-----
```

| MAC Address    | User Name | APID/RID | IP Address   | VLAN |
|----------------|-----------|----------|--------------|------|
| 0001-8500-0001 | -NA-      | 5 /1     | 181.254.5.2  | 1005 |
| 0001-8500-0002 | -NA-      | 5 /1     | 181.254.3.3  | 1003 |
| 0001-8500-0003 | -NA-      | 5 /1     | 181.254.4.4  | 1004 |
| 0001-8500-0004 | -NA-      | 5 /1     | 181.254.6.5  | 1006 |
| 0001-8500-0005 | -NA-      | 5 /1     | 181.254.7.6  | 1007 |
| 0001-8500-0006 | -NA-      | 5 /1     | 181.254.8.7  | 1008 |
| 0001-8500-0007 | -NA-      | 5 /1     | 181.254.10.8 | 1010 |
| 0001-8500-0008 | -NA-      | 5 /1     | 181.254.9.9  | 1009 |

|                |      |   |    |               |      |
|----------------|------|---|----|---------------|------|
| 0001-8500-0009 | -NA- | 5 | /1 | 181.254.0.10  | 1000 |
| 0001-8500-000a | -NA- | 5 | /1 | 181.254.1.11  | 1001 |
| 0001-8500-000b | -NA- | 5 | /1 | 181.254.9.12  | 1009 |
| 0001-8500-000c | -NA- | 5 | /1 | 181.254.10.13 | 1010 |
| 0001-8500-000d | -NA- | 5 | /1 | 181.254.2.14  | 1002 |
| 0001-8500-000e | -NA- | 6 | /1 | 181.254.7.15  | 1007 |
| 0001-8500-000f | -NA- | 5 | /1 | 181.254.6.16  | 1006 |
| 0001-8500-0010 | -NA- | 5 | /1 | 181.254.10.17 | 1010 |
| 0001-8500-0011 | -NA- | 5 | /1 | 181.254.0.18  | 1000 |
| 0001-8500-0012 | -NA- | 5 | /1 | 181.254.10.19 | 1010 |
| 0001-8500-0013 | -NA- | 5 | /1 | 181.254.9.20  | 1009 |
| 0001-8500-0014 | -NA- | 6 | /1 | 181.254.1.21  | 1001 |
| 0001-8500-0015 | -NA- | 6 | /1 | 181.254.3.22  | 1003 |
| 0001-8500-0016 | -NA- | 6 | /1 | 181.254.2.23  | 1002 |
| 0001-8500-0017 | -NA- | 6 | /1 | 181.254.5.24  | 1005 |
| 0001-8500-0018 | -NA- | 6 | /1 | 181.254.1.25  | 1001 |
| 0001-8500-0019 | -NA- | 6 | /1 | 181.254.7.26  | 1007 |
| 0001-8500-001a | -NA- | 6 | /1 | 181.254.3.27  | 1003 |
| 0001-8500-001b | -NA- | 6 | /1 | 181.254.2.28  | 1002 |
| 0001-8500-001c | -NA- | 6 | /1 | 181.254.9.29  | 1009 |
| 0001-8500-001d | -NA- | 6 | /1 | 181.254.8.30  | 1008 |
| 0001-8500-001e | -NA- | 6 | /1 | 181.254.2.31  | 1002 |
| 0001-8500-001f | -NA- | 6 | /1 | 181.254.3.32  | 1003 |
| 0001-8500-0020 | -NA- | 6 | /1 | 181.254.2.33  | 1002 |
| 0001-8500-0021 | -NA- | 6 | /1 | 181.254.0.34  | 1000 |
| 0001-8500-0022 | -NA- | 6 | /1 | 181.254.3.35  | 1003 |
| 0001-8500-0023 | -NA- | 6 | /1 | 181.254.4.36  | 1004 |
| 0001-8500-0024 | -NA- | 6 | /1 | 181.254.4.37  | 1004 |
| 0001-8500-0025 | -NA- | 6 | /1 | 181.254.5.38  | 1005 |
| 0001-8500-0026 | -NA- | 6 | /1 | 181.254.5.39  | 1005 |
| 0001-8500-0027 | -NA- | 6 | /1 | 181.254.8.40  | 1008 |

...略...

# 通过命令 **display wlan statistics client vlan-pool** 查看 VLAN 池 vp1 中分配给无线客户端的 VLAN 的情况。

```
<AC> display wlan statistics client vlan-pool vp1
```

#### VLAN Pool Information

```
-----
VLAN Pool Name      : vp1
VLAN List           : 1000 to 1010
VLANs in Use        : 1000 to 1010
Total Clients        : 128
-----
```

```
-----
VLAN ID             Number of Clients
-----
1000                 12
1001                 12
1002                 12
-----
```

|      |    |
|------|----|
| 1003 | 12 |
| 1004 | 12 |
| 1005 | 11 |
| 1006 | 11 |
| 1007 | 11 |
| 1008 | 11 |
| 1009 | 12 |
| 1010 | 12 |

从上面可以看出，VLAN 池中每个 VLAN 分配的客户端数目几乎相等，很好的平衡了各 VLAN 间的网络负载。

# 通过 **display mac-vlan all** 命令能看到这些客户端都生成了动态的 MAC-VLAN 表项（因为配置了 MAC VLAN 功能）。

```
<AC> display mac-vlan all
```

```
The following MAC VLAN addresses exist:
```

```
S:Static D:Dynamic
```

| MAC ADDR | MASK | VLAN ID | PRIO | STATE |
|----------|------|---------|------|-------|
|----------|------|---------|------|-------|

|                |                |      |   |   |
|----------------|----------------|------|---|---|
| 0001-8500-0046 | ffff-ffff-ffff | 1000 | 0 | D |
| 0001-8500-0041 | ffff-ffff-ffff | 1001 | 0 | D |
| 0001-8500-0001 | ffff-ffff-ffff | 1002 | 0 | D |
| 0001-8500-0002 | ffff-ffff-ffff | 1003 | 0 | D |
| 0001-8500-0042 | ffff-ffff-ffff | 1004 | 0 | D |
| 0001-8500-0004 | ffff-ffff-ffff | 1005 | 0 | D |
| 0001-8500-0007 | ffff-ffff-ffff | 1006 | 0 | D |
| 0001-8500-0008 | ffff-ffff-ffff | 1007 | 0 | D |
| 0001-8500-0043 | ffff-ffff-ffff | 1008 | 0 | D |
| 0001-8500-000a | ffff-ffff-ffff | 1009 | 0 | D |
| 0001-8500-000b | ffff-ffff-ffff | 1010 | 0 | D |
| 0001-8500-000c | ffff-ffff-ffff | 1000 | 0 | D |
| 0001-8500-000d | ffff-ffff-ffff | 1001 | 0 | D |
| 0001-8500-0047 | ffff-ffff-ffff | 1002 | 0 | D |
| 0001-8500-0045 | ffff-ffff-ffff | 1004 | 0 | D |
| 0001-8500-0044 | ffff-ffff-ffff | 1005 | 0 | D |
| 0001-8500-0048 | ffff-ffff-ffff | 1003 | 0 | D |
| 0001-8500-0049 | ffff-ffff-ffff | 1006 | 0 | D |

```
.....
```

```
Total MAC VLAN address count:128
```

# 让某些无线客户快速地下线再上线（间隔不超过 3 分钟），重新上线后这些无线客户端会继承上一次的 VLAN，但 **display wlan statistics client vlan-pool** 不会再对这些客户端进行统计。例如本例中让这 128 个客户端重新上线一次，再次查看 **vlan-pool** 统计表，由于都继承了上一次的 VLAN，不属于地址池重新分配，故而统计出来的值为 0。

```
<AC> display wlan statistics client vlan-pool vp1
```

```
VLAN Pool Information
```

|                |                |
|----------------|----------------|
| VLAN Pool Name | : vp1          |
| VLAN List      | : 1000 to 1010 |

```
VLANs in Use      :  
Total Clients     : 0
```

```
-----  
VLAN ID           Number of Clients  
-----
```

## 3.6 配置文件

- AC:

```
#  
vlan 100  
#  
vlan 200  
#  
vlan 1000 to 1010  
#  
wlan vlan-pool vp1  
    vlan-id 1000 to 1010  
#  
wlan service-template 1 clear  
    ssid service  
    bind WLAN-ESS 1  
    service-template enable  
#  
interface Vlan-interface100  
    ip address 181.254.100.1 255.255.0.0  
#  
interface Vlan-interface1000  
    ip address 181.254.0.1 255.255.255.0  
#  
interface Vlan-interface1001  
    ip address 181.254.1.1 255.255.255.0  
#  
interface Vlan-interface1002  
    ip address 181.254.2.1 255.255.255.0  
#  
interface Vlan-interface1003  
    ip address 181.254.3.1 255.255.255.0  
#  
interface Vlan-interface1004  
    ip address 181.254.4.1 255.255.255.0  
#  
interface Vlan-interface1005  
    ip address 181.254.5.1 255.255.255.0  
#  
interface Vlan-interface1006  
    ip address 181.254.6.1 255.255.255.0  
#
```



```

interface Vlan-interface1007
 ip address 181.254.7.1 255.255.255.0
#
interface Vlan-interface1008
 ip address 181.254.8.1 255.255.255.0
#
interface Vlan-interface1009
 ip address 181.254.9.1 255.255.255.0
#
interface Vlan-interface1010
 ip address 181.254.10.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 1000 to 1010
 undo port trunk permit vlan 1
 port trunk pvid vlan 100
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 1000 to 1010 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
#
wlan ap officeap1 model WA2620E-AGN id 1
 serial-id 210235A29G007C000020
 radio 1
 service-template 1 vlan-pool vp1
 radio enable
 radio 2
#
wlan ap officeap2 model WA2620E-AGN id 2
 serial-id 210235A29G007C000021
 radio 1
 service-template 1 vlan-pool vp1
 radio enable
 radio 2
#
ip route-static 8.0.0.0 255.0.0.0 8.181.1.2
#
• Switch:
#
vlan 100
#
vlan 1000 to 1010
#
interface GigabitEthernet1/0/1

```

```
port link-type trunk
port trunk permit vlan 100 1000 to 1010
undo port trunk permit vlan 1
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/4
port link-type access
port access vlan 100
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 基于客户端的无线捕获典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                            |    |
|----------------------------|----|
| 1 简介.....                  | 1  |
| 2 配置前提 .....               | 1  |
| 3 配置举例 .....               | 1  |
| 3.1 组网需求 .....             | 1  |
| 3.2 配置思路 .....             | 2  |
| 3.3 配置注意事项 .....           | 2  |
| 3.4 配置步骤 .....             | 2  |
| 3.4.1 AC 的配置 .....         | 2  |
| 3.4.2 Switch 的配置 .....     | 5  |
| 3.4.3 AAA server 的配置 ..... | 6  |
| 3.5 验证配置 .....             | 8  |
| 3.6 配置文件 .....             | 9  |
| 4 相关资料 .....               | 11 |

# 1 简介

本文档介绍 WLAN 基于客户端的无线捕获报文记录的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 AAA、802.1X 和 WLAN 特性。

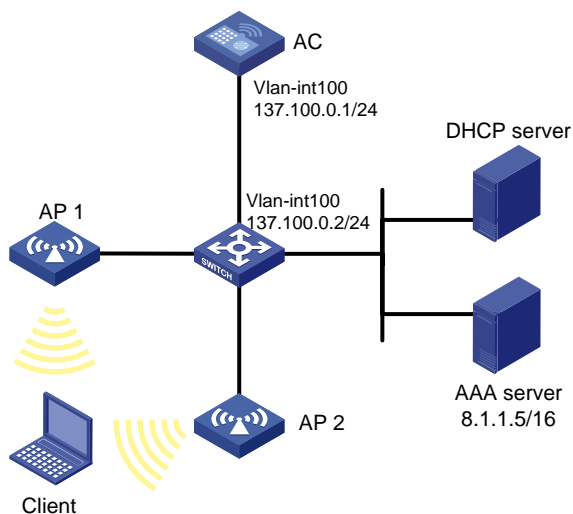
## 3 配置举例

### 3.1 组网需求

如图 1 所示，无线客户端首先在 AP 1 上线并漫游至 AP 2。要求：

- 对 Client 进行 EAP 中继方式的 802.1X 认证。
- 对 Client 和 AC 间的传输数据进行加密。
- 通过开启基于客户端的无线报文捕获功能，捕获客户端发送和接收到的与客户端上线或状态更新相关的管理、控制与数据报文。
- 将捕获的报文记录在 office.dmp 的文件中。

图1 基于客户端的无线捕获典型配置组网图



## 3.2 配置思路

- 由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。
- 为了防止用户通过恶意假冒其它域账号从本端口接入网络，配置端口的强制认证域。
- 为了对 Client 和 AC 间的传输数据进行加密，采用 AES-CCMP 加密套件。

## 3.3 配置注意事项

- 目前，配置基于客户端的无线捕获的 ACL 时，设备只支持二层 ACL，且只支持源 MAC 地址的匹配，不支持目地 MAC 匹配。
- 捕获到的报文将保存在 AC 的文件系统中，如果 AC 的存储空间小于 2M，将无法继续保存。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 由于端口安全特性通过多种安全模式提供了 802.1X 认证的扩展和组合应用，因此在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 接口和路由信息

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface101] ip address 137.100.0.1 24
[AC-Vlan-interface101] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置默认路由。

```
[AC] ip route-static 0.0.0.0 0 137.100.0.2
```

# 配置 AC 与 Switch 连接的 GigabitEthernet1/0/1 接口的属性为 trunk，禁止 VLAN 1 通过，允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface GigabitEthernet1/0/1
```

```
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置 802.1X 认证服务

# 使能端口安全。

```
[AC] port-security enable
```

# 配置 802.1X 用户的认证方式为 EAP。

```
[AC] dot1x authentication-method eap
```

# 创建 RADIUS 方案 office。

```
[AC] radius scheme office
```

# 配置主认证 AAA 服务器的 IP 地址 8.1.1.5，主计费 AAA 服务器的 IP 地址 8.1.1.5。

```
[AC-radius-office] primary authentication 8.1.1.5
```

```
[AC-radius-office] primary accounting 8.1.1.5
```

# 配置系统与 AAA 认证服务器交互报文时的共享密钥为 123456789，与 AAA 计费服务器交互报文时的共享密钥为 123456789。

```
[AC-radius-office] key authentication 123456789
```

```
[AC-radius-office] key accounting 123456789
```

# 配置 AC 发送给 AAA 服务器的用户名不带 ISP 域名。

```
[AC-radius-office] user-name-format without-domain
```

# 配置 AC 发送至 AAA 服务器的报文使用的源 IP 地址为 137.100.0.1。

```
[AC-radius-office] nas-ip 137.100.0.1
```

```
[AC-radius-office] quit
```

# 创建 office 域并进入其视图。

```
[AC] domain office
```

# 为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] authentication lan-access radius-scheme office
```

# 为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] authorization lan-access radius-scheme office
```

# 为 lan-access 用户配置计费为 none，不计费。

```
[AC-isp-office] accounting lan-access none
```

```
[AC-isp-office] quit
```

## (3) 配置无线服务

# 创建 WLAN-ESS1 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 配置 WLAN-ESS1 口开启 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

# 在接口 WLAN-ESS1 上配置 802.1X 用户的强制认证域 office。

```

[AC-WLAN-ESS1] dot1x mandatory-domain office
# 配置端口安全模式为 userlogin-secure-ext，并使能端口 11key 类型的密钥协商功能。
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 关闭 802.1X 多播触发功能和在线用户握手功能。
[AC-WLAN-ESS1] undo dot1x multicast-trigger
[AC-WLAN-ESS1] undo dot1x handshake
[AC-WLAN-ESS1] quit
# 创建 crypto 类型的服务模板 1。
[AC] wlan service-template 1 crypto
# 设置当前服务模板的 SSID 为 service1。
[AC-wlan-st-1] ssid service1
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 配置加密套件为 AES-CCMP。
[AC-wlan-st-1] cipher-suite ccmp
# 设置在 AP 发送信标和探查响应帧时携带 RSN IE，并使能服务模板。
[AC-wlan-st-1] security-ie rsn
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(4) 配置射频接口并绑定服务模板
# 创建 AP 1 的模板，名称为 officeap1，型号名称选择 WA2620E-AGN，并配置其序列号。
[AC] wlan ap officeap1 model WA2620E-AGN
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
# 设置 AP 1 的 radio 2 工作模式为 dot11gn。
[AC-wlan-ap-officeap1] radio 2 type dot11gn
# 将在 AC 上配置的服务模板 1 与射频 2 进行关联，Client 通过服务模板 1 接入 VLAN 300。
[AC-wlan-ap-officeap1-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap1-radio-2] radio enable
[AC-wlan-ap-officeap1-radio-2] quit
[AC-wlan-ap-officeap1] quit
# 创建 AP 2 的模板，名称为 officeap2，型号名称选择 WA2620E-AGN，并配置其序列号。
[AC] wlan ap officeap2 model WA2620E-AGN
[AC-wlan-ap-officeap2] serial-id 21023529G007C000021
# 设置 AP 2 的 radio 2 工作模式为 dot11gn。
[AC-wlan-ap-officeap2] radio 2 type dot11gn
# 将在 AC 上配置的服务模板 1 与射频 2 进行关联，Client 通过服务模板 1 接入 VLAN 300。
[AC-wlan-ap-officeap2-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap2-radio-2] radio enable
[AC-wlan-ap-officeap2-radio-2] quit
[AC-wlan-ap-officeap2] quit
(5) 配置无线报文捕获

```



# 配置 ACL 4000，匹配客户端的源 MAC 地址。

```
[AC] acl number 4000
[AC-acl-ethernetframe-4000] rule 1 permit source-mac 0015-00ef-ac23 ffff-ffff-ffff
[AC-acl-ethernetframe-4000] quit
```

# 配置 AP 捕获报文的记录文件名为 office。

```
[AC] wlan capture file-name office
```

# 配置客户端报文捕获的匹配条件为 ACL 4000，并开启报文捕获。

```
[AC] wlan capture start client acl 4000
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface GigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

# 在 Switch 上配置接口 VLAN 100 的 IP 地址为 137.100.0.2/24。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 137.100.0.2 255.255.255.0
[Switch-Vlan-interface100] quit
```

### 3.4.3 AAA server 的配置



说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)），说明 RADIUS 服务器的基本配置。

# 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置认证、计费共享密钥为 123456789，其它保持缺省配置；
- 选择或手工增加接入设备，添加 IP 地址为 137.100.0.1 的接入设备。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 帮助

接入配置

认证端口 \*

1812

计费端口 \*

1813

组网方式

不启用混合组网

业务类型

LAN接入业务

接入设备类型

H3C(General)

接入设备分组

无

共享密钥 \*

.....

确认共享密钥 \*

.....

业务分组

未分组

设备列表

选择

手工增加

全部清除

| 设备名称 | 设备IP地址      | 设备型号 | 备注 | 删除 |
|------|-------------|------|----|----|
|      | 137.100.0.1 |      |    |    |

共有1条记录。

确定

取消

# 增加接入策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击<增加>按钮，进入增加接入策略页面。

- 设置接入策略名为 office；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证。

图3 增加接入策略页面

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略 帮助

基本信息

接入策略名 \*

office

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

启用RSA认证

证书认证

不启用

启用EAP证书认证

启用WAP证书认证

认证证书子类型

EAP-PEAP认证

认证证书子类型

MS-CHAPV2认证

下发VLAN

下发用户组

下发User Profile

下发ACL

认证绑定信息

绑定接入设备IP

绑定接入设备端口

绑定VLAN

绑定QinQ双VLAN

绑定用户IP地址

绑定用户MAC地址

绑定IMSI号码

绑定计算机名称

计算机绑定域

用户必须登录到域

绑定无线SSID

绑定接入设备序列号

启用终端MAC地址控制

启用终端硬盘序列号控制

启用无线SSID控制

# 增加接入服务。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 设置服务名为 **office**；
- 选择缺省接入策略为 **office**，其他保持缺省配置。

图4 增加接入服务页面

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

基本信息

服务名 \*

office

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

office

缺省安全策略 \*

不使用

缺省内网外联配置 \*

不使用

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 ( PC )

服务描述

可申请

Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 安全策略 | 私有属性下发策略 | 内网外联配置 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|------|----------|--------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |      |          |        |        |     |    |    |

确定

取消

# 增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 单击<增加用户>添加用户 **office**，证件号码 **123456**；
- 添加帐号名为 **office**，密码为 **123456**；
- 选中刚才配置的服务 **office**。

图5 增加接入用户

用户姓名 \*

office

选择

增加用户

帐号名 \*

office

☐ 预开用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                        | 服务后缀 | 缺省安全策略  | 状态  | 分配IP地址 |
|--------------------------------------------|------|---------|-----|--------|
| <input type="checkbox"/> 802.1x            |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> 802.1x-eap        |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> l2l3              |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> l2l3-802.1x       |      | 不使用     | 可申请 |        |
| <input type="checkbox"/> mpc_ead           |      | mpc_ead | 可申请 |        |
| <input type="checkbox"/> mpc_peap          |      | 不使用     | 可申请 |        |
| <input checked="" type="checkbox"/> office |      | 不使用     | 可申请 |        |

3.5 验证配置

```
# 当客户端在 AP 1 上线并认证成功后，在 AC 上停止报文捕获。
[AC] wlan capture stop
Warning: Save the WLAN capture information to an archive file. Continue? [Y/N]:y
# 查看文件系统目录，找到记录捕获信息的文件 office.dmp。
<AC> dir
Directory of cfa0:/

0      drw-      -   Feb 12 2013 11:05:08   logfile
1      -rw-      2530  Oct 11 2013 09:31:10   startup.cfg
2      -rw-      349   Feb 12 2013 13:15:18   system.xml
3      -rw-      523   Nov 19 2013 14:12:22   office.dmp

# 通过 FTP 等方式将 office.dmp 下载到本地计算机，可以通过报文解析工具查看捕获到的 Client
和 AC 之间从捕获开始以来所有的报文。
# 修改捕获报文的记录文件名为 roam。
[AC] wlan capture file-name roam
# 再次开启报文捕获，操作客户端从 AP 1 漫游至 AP 2。
[AC] wlan capture start client acl 4000
# 客户端漫游至 AP 2 上线并认证成功后，停止报文捕获，得到记录捕获信息的文件 roam.dmp。
[AC] wlan capture stop
Warning: Save the WLAN capture information to an archive file. Continue? [Y/N]:y
# 通过 FTP 等方式将 roam.dmp 下载到本地计算机，可以通过报文解析工具查看 Client 在漫游过程
中与 AC 之间交互的所有报文。
```

## 3.6 配置文件

- AC:

```
#
port-security enable
#
dot1x authentication-method eap
#
wlan capture file-name office
#
acl number 4000
rule 1 permit source-mac 0015-00ef-ac23 ffff-ffff-ffff
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
primary authentication 8.1.1.5
primary accounting 8.1.1.5
key authentication cipher $c$3$SjWMEAjbtjqCC9+XHRLYhNZOSJ6bBN/7K3HBEA==
key accounting cipher $c$3$Oj5WtaBGNaZb9s+R0Y/z0yKMG4fZcS0LuOUeOw==
user-name-format without-domain
nas-ip 137.100.0.1
#
domain office
authentication lan-access radius-scheme office
authorization lan-access radius-scheme office
accounting lan-access none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 crypto
ssid servicel
bind WLAN-ESS 1
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200 300
#
```

```

interface Vlan-interface100
 ip address 137.100.0.1 255.255.255.0
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain office
 undo dot1x multicast-trigger
#
wlan ap officeap1 model WA2620E-AGN id 1
 serial-id 21023529G007C000020
 radio 1
 radio 2
 service-template 1 vlan-id 300
 radio enable
#
wlan ap officeap2 model WA2620E-AGN id 2
 serial-id 21023529G007C000021
 radio 1
 radio 2
 service-template 1 vlan-id 300
 radio enable
#
ip route-static 0.0.0.0 0.0.0.0 137.100.0.2
#

```

- **Switch:**

```

#
vlan 100
#
vlan 300
#
interface Vlan-interface100
 ip address 137.100.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 300
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge

```

```
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 基于用户的 WIAA 安全控制典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

|                               |    |
|-------------------------------|----|
| 1 简介.....                     | 1  |
| 2 配置前提 .....                  | 1  |
| 3 使用限制 .....                  | 1  |
| 4 配置举例 .....                  | 1  |
| 4.1 组网需求 .....                | 1  |
| 4.2 配置思路 .....                | 2  |
| 4.3 配置注意事项 .....              | 2  |
| 4.4 配置步骤 .....                | 2  |
| 4.4.1 AC 的配置 .....            | 2  |
| 4.4.2 Switch 的配置 .....        | 6  |
| 4.4.3 RADIUS Server 的配置 ..... | 7  |
| 4.5 验证配置 .....                | 14 |
| 4.6 配置文件 .....                | 15 |
| 5 相关资料 .....                  | 18 |

# 1 简介

本文档介绍了基于用户的 WIAA 安全控制网络的典型配置举例。

WIAA (Wireless Intelligent Application Aware, 无线智能业务感知), 可提供基于无线端口的访问控制, 通过在无线接口上的出方向上应用防火墙的 **Packet-Filter**, 入方向上应用 **ASPF** 策略, 能够拒绝有线网络直接访问无线用户, 但不影响无线用户的访问权限, 确保了无线网络内的安全。

## 2 配置前提

本文档不严格与具体软、硬件版本对应, 如果使用过程中与产品实际情况有差异, 请参考相关产品手册, 或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证, 配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置, 为了保证配置效果, 请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解无线 WIAA 特性。

## 3 使用限制

本文涉及的包过滤防火墙和 **ASPF** 功能需要用户购买 **License**, 并完成注册之后才能使用。**License** 可以通过购买特性软件授权书获得, 授权书上提供了注册 WIAA 特性需要使用的 **License** 授权码及特性功能说明。详细的操作流程, 请参见《H3C WX 系列无线控制产品 **License** 激活申请和注册操作指导》, 添加 **License** 的相关配置请参见“基础配置指导”中的“**License** 管理配置”。

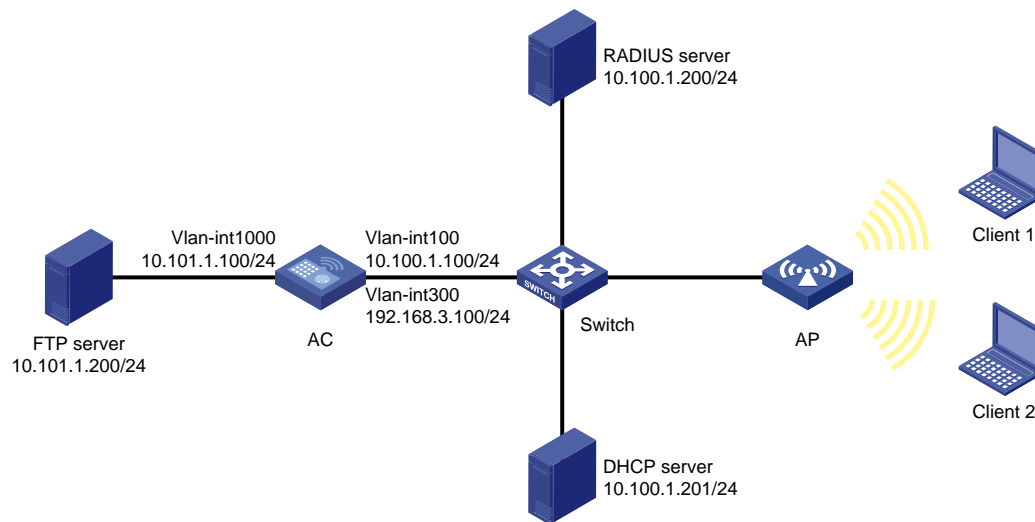
## 4 配置举例

### 4.1 组网需求

如[图 1](#)所示, 某公司部署 **WLAN** 网络, 使公司内部员工和外部来访人员均可以通过 **WLAN** 接入访问公司内网, 要求对接入 **WLAN** 的无线用户采用 **802.1X** 认证, 在限制外部来访者对 **FTP** 服务器的访问的同时要限制 **FTP** 服务器对无线用户的访问。具体应用需求如下:

- 无线用户 **Client 1** 是公司员工, 接入 **WLAN** 后可访问 **FTP** 服务器。
- 无线用户 **Client 2** 是外部来访人员, 接入 **WLAN** 后不能访问 **FTP** 服务器。
- **AC** 上配置防火墙, 限制有线网络中的 **FTP server** 访问 **WLAN**, 从而保证 **WLAN** 的安全。

图1 基于用户的 WIAA 安全控制网络配置组网图



## 4.2 配置思路

- 为了让 WLAN 接入用户有不同的访问权限，需要定义不同的 User-Profile，从而可以根据用户接入认证时使用的用户名为 Client 分配不同的访问权限。
- 为了限制有线网络中的 FTP server 主动访问 WLAN，需要创建 ACL 规则，并应用于防火墙 Packet-Filter。
- 为了保证无线客户端 Client 向 FTP server 发送的请求报文，以及 FTP server 对 Client 的应答报文可以正常通过 AC，需要在 AC 上创建防火墙 ASPF 策略。
- 为了限制有线网络中的 FTP server 对 WLAN 访问，在 User-Profile 中 outbound 方向需要应用 Packet-Filter 进行流量的过滤。

## 4.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 确保 User-Profile 中的出方向应用防火墙 Packet-Filter、入方向应用 ASPF 策略。
- 关闭 ALG 会使 ASPF 对应用层协议的功能失效（ALG 功能默认开启）。

## 4.4 配置步骤

### 4.4.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
```

```

[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.100.1.100 255.255.255.0
[AC-Vlan-interface100] quit
# 创建 VLAN 300 及其对应的 VLAN 接口，并为该接口配置 IP 地址。VLAN 300 将作为 WLAN-ESS
接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN。
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 192.168.3.100 255.255.255.0
[AC-Vlan-interface300] quit
# 创建 VLAN 1000 及其对应的 VLAN 接口，并为该接口配置 IP 地址。VLAN 1000 将作为 AC 和
FTP 服务器通信的 VLAN。
[AC] vlan 1000
[AC-vlan1000] quit
[AC] interface vlan-interface 1000
[AC-Vlan-interface1000] ip address 10.101.1.100 255.255.255.0
[AC-Vlan-interface1000] quit
# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/2 接口的链路类型为 Trunk，当前 Trunk 口的 PVID
为 100，允许 VLAN 100 和 VLAN 300 通过。
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] port link-type trunk
[AC-GigabitEthernet1/0/2] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/2] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/2] quit
# 创建 WLAN-ESS 1 接口，并设置端口的链路类型为 Hybrid。
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 300，禁止 VLAN 1 通过并允许 VLAN 300 不带 tag 通过。
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 300 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 300
# 在 Hybrid 端口上使能 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit

```

## (2) 配置 ACL

```

# 为 ACL 3000 创建规则，拒绝所有 IP 报文通过，用于限制有线网络主动访问 WLAN。
[AC] acl number 3000
[AC-acl-adv-3000] rule deny ip
[AC-acl-adv-3000] quit
# 为 ACL 3001 创建规则，允许所有 IP 报文通过，并配置描述信息为 “group_staff”，用于使公司
员工可以访问内网。
[AC] acl number 3001
[AC-acl-adv-3001] description group_staff
[AC-acl-adv-3001] rule permit ip
[AC-acl-adv-3001] quit

```

# 为 ACL 3002 创建规则，允许所有 IP 报文通过，但拒绝目的端口为 FTP 的报文，并配置描述信息为 “group\_visitor”，用于限制外部来访人员访问内网。

```
[AC] acl number 3002
[AC-acl-adv-3002] description group_visitor
[AC-acl-adv-3002] rule deny tcp destination-port eq ftp
[AC-acl-adv-3002] rule permit ip
[AC-acl-adv-3002] quit
```

(3) 创建 ASPF 策略 1，缺省情况下，ASPF 检测处于开启状态，故采用缺省配置。

```
[AC] aspf-policy 1
[AC-aspf-policy-1] quit
```

(4) 配置基于用户的无线防火墙策略

# 创建名为 group\_visitor 的 User-Profile，用于定义外部来访者的防火墙策略。

```
[AC] user-profile group_visitor
# 使用 ACL 3002 对入方向的报文进行过滤。
[AC-user-profile-group_visitor] firewall packet-filter 3002 inbound
# 使用 ACL 3000 对出方向的报文进行过滤。
[AC-user-profile-group_visitor] firewall packet-filter 3000 outbound
# 对入方向的报文应用 ASPF 策略 1。
```

```
[AC-user-profile-group_visitor] firewall aspf 1 inbound
[AC-user-profile-group_visitor] quit
```

# 使能名为 group\_visitor 的 User-Profile。

```
[AC] user-profile group_visitor enable
```

# 创建名为 group\_staff 的 User-Profile，用于定义公司员工的防火墙策略。

```
[AC] user-profile group_staff
# 使用 ACL 3001 对入方向的报文进行过滤。
[AC-user-profile-group_staff] firewall packet-filter 3001 inbound
# 使用 ACL 3000 对出方向的报文进行过滤。
[AC-user-profile-group_staff] firewall packet-filter 3000 outbound
# 对入方向的报文应用 ASPF 策略 1。
```

```
[AC-user-profile-group_staff] firewall aspf 1 inbound
[AC-user-profile-group_staff] quit
```

# 使能名为 group\_staff 的 User-Profile。

```
[AC] user-profile group_staff enable
```

# 全局下使能防火墙。

```
[AC] firewall enable
```

(5) 配置 802.1X 认证

# 开启端口安全。

```
[AC] port-security enable
```

# 配置 802.1X 用户的认证方式为 EAP。

```
[AC] dot1x authentication-method eap
```

# 创建名为 office 的 RADIUS 方案，并指定 RADIUS 服务器的类型为 extended。

```
[AC] radius scheme office
[AC-radius-office] server-type extended
```

# 配置主认证 RADIUS 服务器的 IP 地址为 10.100.1.200。

```

[AC-radius-office] primary authentication 10.100.1.200
# 认证报文的共享密钥设置为明文 1234。
[AC-radius-office] key authentication 1234
# 指定发送给 RADIUS 服务器的用户名不得携带域名。
[AC-radius-office] user-name-format without-domain
[AC-radius-office] quit
# 创建名为 office 的 ISP 域，并进入其视图。
[AC] domain office
# 配置 lan-access 用户使用 RADIUS 方案 office 进行认证和授权，不对用户使用的网络服务进行计费。
[AC-isp-office] authentication lan-access radius-scheme office
[AC-isp-office] accounting lan-access none
[AC-isp-office] authorization lan-access radius-scheme office
[AC-isp-office] quit
# 在接口 WLAN-ESS 1 上配置 802.1X 用户的强制认证域 office。
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] dot1x mandatory-domain office
# 配置端口安全模式为 userlogin-secure-ext，并使能端口 11key 类型的密钥协商功能。
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 关闭 802.1X 多播触发功能和在线用户握手功能。
[AC-WLAN-ESS1] undo dot1x multicast-trigger
[AC-WLAN-ESS1] undo dot1x handshake
[AC-WLAN-ESS1] quit
(6) 配置无线服务
# 创建 crypto 类型的服务模板 1。
[AC] wlan service-template 1 crypto
# 设置当前服务模板的 SSID 为 service，加密方式为 TKIP 和 AES-CCMP。
[AC-wlan-st-1] ssid service
[AC-wlan-st-1] authentication-method open-system
[AC-wlan-st-1] cipher-suite tkip
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
# 将 WLAN-ESS 1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(7) 配置射频接口并绑定服务模板
# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。
[AC] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。

```

```
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
```

#### 4.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 并允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access, 并允许 VLAN 100 通过, 并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口的链路类型为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 RADIUS server 相连的 GigabitEthernet1/0/4 接口的链路类型为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

### 4.4.3 RADIUS Server 的配置



说明

下面以 IMC 为例（使用 IMC 版本为：iMC PLAT 7.0 (E0202)、iMC WSM 7.0 (E0202)），说明 Radius Server 的基本配置。

#### # 增加接入设备

登录进入 IMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入“接入设备配置”页面，在该页面中单击<增加>按钮，进入“增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“1234”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择接入设备类型为“H3C(General)”；
- 在设备列表中，单击<手工增加>按钮，添加 IP 地址为 10.100.1.100 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

 用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 

接入配置

认证端口 \*

1812

计费端口 \*

1813

组网方式

不启用混合组网

业务类型

LAN接入业务

接入设备类型

H3C(General)

接入设备分组

无

共享密钥 \*

....

确认共享密钥 \*

....

业务分组

未分组

设备列表

选择

手工增加

全部清除

| 设备名称 | 设备IP地址       | 设备型号 | 备注 | 删除                                                                                    |
|------|--------------|------|----|---------------------------------------------------------------------------------------|
|      | 10.100.1.100 |      |    |  |

共有1条记录。

确定

取消

#### # 增加公司员工的接入策略

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入“接入策略管理”页面，单击“增加”按钮，进入“增加接入策略”页面。

- 接入策略名为“dot1x\_staff”，该名称可以自行定义；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证；
- 选择下发 User Profile，并输入 AC 对应的 User-Profile 名“group\_staff”。



- 其他配置采用缺省配置；
- 单击<确定>按钮完成操作。

图3 增加公司员工的接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略 帮助

基本信息

接入策略名 \*

dot1x\_staff

业务分组 \*

未分组

描述

授权信息

接入时段

无

?

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☐ 不启用
☒ EAP证书认证
☐ WAP证书认证

认证证书类型

EAP-PEAP认证

认证证书子类型

MS-CHAPV2认证

下发VLAN

☒ 下发User Profile

group\_staff

下发用户组

?

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMS号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 禁用Windows可溶解客户端

网络故障时自动重连

自动重连间隔(分钟)

30

自动重连次数

3

违规处理模式

☒ 下线
☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式

☒ 不限制
☐ 必须静态设置
☐ 必须动态获取

确定

取消

### # 增加来访人员的接入策略

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入“接入策略管理”页面，单击“增加”按钮，进入“增加接入策略”页面。

- 接入策略名为“dot1x\_visitor”，该名称可以自行定义；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证；
- 选择下发 User Profile，并输入 AC 对应的 User-Profile 名“group\_visitor”。
- 其他配置采用缺省配置；
- 单击<确定>按钮完成操作。

图4 增加来访人员的接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

帮助

基本信息

接入策略名 \*

dot1x\_visitor

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☐ 不启用 ☒ EAP证书认证 ☐ WAP证书认证

认证证书类型

EAP-PEAP认证

认证证书子类型

MS-CHAPV2认证

下发VLAN

下发用户组

☒ 下发User Profile

group\_visitor

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Windows可溶解客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔(分钟) 30

自动重连次数 3

违规处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式

☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定

取消

# 增加公司员工的接入服务

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入“接入服务管理”页面，点击<增加>按钮，进入“增加接入服务”页面。

- 输入服务名“staff”，该名称可以自行定义；
- 业务分组“未分组”；
- 缺省接入策略选择“dot1x\_staff”，即上一步配置的公司员工接入策略名；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 增加公司员工的接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

帮助

基本信息

服务名 \*

staff

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

dot1x\_staff

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 (PC

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

# 增加来访人员的接入服务

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入“接入服务管理”页面，点击<增加>按钮，进入“增加接入服务”页面。

- 输入服务名“visitor”，该名称可以自行定义；
- 业务分组“未分组”；
- 缺省接入策略选择“dot1x\_visitor”，即上一步配置的来访人员接入策略名；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加来访人员的接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

帮助

基本信息

服务名 \*

visitor

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

dot1x\_visitor

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 (PC

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

# 配置公司员工接入用户

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入“接入用户”页面，在该页面中单击<增加>按钮，进入“增加接入用户”页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“staff”；
- 输入证件号码“staff”；

- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图7 增加用户

增加用户

基本信息

用户姓名 \*

staff

✓

证件号码 \*

staff

✓

检查是否可用

通讯地址

电话

?

电子邮件

?

用户分组 \*

未分组

👤

确定

取消

在“增加接入用户”页面，按如下方式配置。

- 输入账号名 “staff”；
- 输入密码 “staff” ；
- 接入服务选择 “staff” ；
- 其他配置保持默认；
- 单击<确定>按钮完成操作。

图8 增加公司员工接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

staff

选择

增加用户

帐号名 \*

staff

☐ 预开用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                       | 服务后缀 | 状态  | 分配IP地址 |
|-------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> staff |      | 可申请 |        |
| <input type="checkbox"/> visitor          |      | 可申请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线SSID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

IP地址

MAC地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

# 配置来访人员接入用户

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入“接入用户”页面，在该页面中单击<增加>按钮，进入“增加接入用户”页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“visitor”；
- 输入证件号码“visitor”；
- 单击<检查是否可用>按钮；
- 如用户姓名和证件号码可用，单击<确定>按钮完成操作。

图9 增加用户

增加用户

基本信息

用户姓名 \*

visitor

证件号码 \*

visitor

检查是否可用

通讯地址

电话

电子邮件

用户分组 \*

未分组

确定

取消

在“增加接入用户”页面，按如下方式配置。

- 输入账号名“visitor”；
- 输入密码“visitor”；
- 接入服务选择“visitor”；
- 其他配置保持默认；
- 单击<确定>按钮完成操作。

图10 增加来访人员接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

visitor

选择

增加用户

帐号名 \*

visitor

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数里限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                         | 服务后缀 | 状态  | 分配IP地址 |
|---------------------------------------------|------|-----|--------|
| <input type="checkbox"/> staff              |      | 可申请 |        |
| <input checked="" type="checkbox"/> visitor |      | 可申请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线SSID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

IP地址

MAC地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

4.5 验证配置

(1) 公司来访者接入 WLAN 后，验证能否访问 FTP 服务器。从访问结果可以看出，外部访问者接入无线局域网后不能访问 FTP 服务器，WIAA 起到了保护公司网络的作用，公司员工接入无线局域网后可以访问 FTP 服务器，不会影响到正常的工作。

# 在来访用户 Client 2 上访问 FTP 服务器，访问失败。

```
D:\> ftp 10.101.1.200
ftp>
```

# 在公司员工用户 Client 1 上访问 FTP 服务器，可以成功访问。

```
D:\> ftp 10.101.1.200
```

```
连接到 10.101.1.200。
220 FTP service ready.
用户(10.101.1.200:(none)): admin
331 Password required for admin.
密码:
230 User logged in.
```

(2) FTP 服务器处于 AC 的上行网络，验证 FTP 服务器能否访问无线用户 Client 1 和 Client 2，即验证 AC 的上行网络能否直接访问无线局域网。

# 在 FTP 服务器上 ping 无线用户 Client 1。

```
D:\> ping 192.168.3.2
```

```
Pinging 192.168.3.2 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 192.168.3.2:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

# 在 FTP 服务器上 ping 无线用户 Client 2。

```
D:\> ping 192.168.3.3
```

```
Pinging 192.168.3.3 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 192.168.3.2:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

# 从 ping 的结果看出，AC 的上行网络不能直接访问 WLAN，从而保证了 WLAN 的安全。

## 4.6 配置文件

- AC 的配置文件:

```
#
 firewall enable
#
 port-security enable
#
 dot1x authentication-method eap
#
acl number 3000
 rule 0 deny ip
```



```

acl number 3001
  description group_staff
  rule 0 permit ip
acl number 3002
  description group_visitor
  rule 0 deny tcp destination-port eq ftp
  rule 5 permit ip
#
vlan100
#
vlan300
#
vlan1000
#
radius scheme office
  server-type extended
  primary authentication 10.100.1.200
  key authentication cipher $c$3$valbiQIfMbLyB65r00evDgE3Tus0/Rc=
  user-name-format without-domain
#
Domain office
  authentication lan-access radius-scheme office
  accounting lan-access none
  authorization lan-access radius-scheme office
  access-limit disable
  state active
  idle-cut disable
  self-service-url disable
#
aspf-policy 1
#
wlan service-template 1 crypto
  ssid service
  bind WLAN-ESS 1
  cipher-suite tkip
  cipher-suite ccmp
  security-ie rsn
  service-template enable
#
user-profile group_staff
  firewall packet-filter 3001 inbound
  firewall packet-filter 3000 outbound
  firewall aspf 1 inbound
user-profile group_visitor
  firewall packet-filter 3002 inbound
  firewall packet-filter 3000 outbound
  firewall aspf 1 inbound
#

```

```

interface Vlan-interface100
 ip address 10.100.1.100 255.255.255.0
#
interface Vlan-interface300
 ip address 192.168.3.100 255.255.255.0
#
interface Vlan-interface1000
 ip address 10.101.1.100 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 100 300
 port trunk pvid vlan 100
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 300 untagged
 port hybrid pvid vlan 300
 mac-vlan enable
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 1lkey
 undo dot1x handshake
 dot1x mandatory-domain 1x
 undo dot1x multicast-trigger
#
wlan ap officeap model WA2620E-AGN id 1
 serial-id 21023529G007C000020
 radio 1
 radio 2
 service-template 1
 radio enable
#
user-profile group_staff enable
 user-profile group_visitor enable
#

```

- Switch 的配置文件:

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 300
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2

```

```
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
#
interface GigabitEthernet1/0/4
port link-type access
port access vlan 100
#
```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“ACL 和 QoS 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“ACL 和 QoS 命令参考”。

# AP 负载均衡典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |    |
|------------------------|----|
| 1 简介.....              | 1  |
| 2 配置前提 .....           | 1  |
| 3 会话模式的负载均衡配置举例 .....  | 1  |
| 3.1 组网需求 .....         | 1  |
| 3.2 配置思路 .....         | 2  |
| 3.3 配置注意事项.....        | 2  |
| 3.4 配置步骤 .....         | 2  |
| 3.4.1 AC 的配置 .....     | 2  |
| 3.4.2 Switch 的配置 ..... | 4  |
| 3.5 验证配置 .....         | 5  |
| 3.6 配置文件 .....         | 5  |
| 4 流量模式的负载均衡配置举例 .....  | 6  |
| 4.1 组网需求 .....         | 6  |
| 4.2 配置思路 .....         | 7  |
| 4.3 配置注意事项.....        | 7  |
| 4.4 配置步骤 .....         | 7  |
| 4.4.1 AC 的配置 .....     | 7  |
| 4.4.2 Switch 的配置 ..... | 9  |
| 4.5 验证配置 .....         | 10 |
| 4.6 配置文件 .....         | 10 |
| 5 相关资料 .....           | 12 |

# 1 简介

本文档介绍了 AP 负载均衡配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

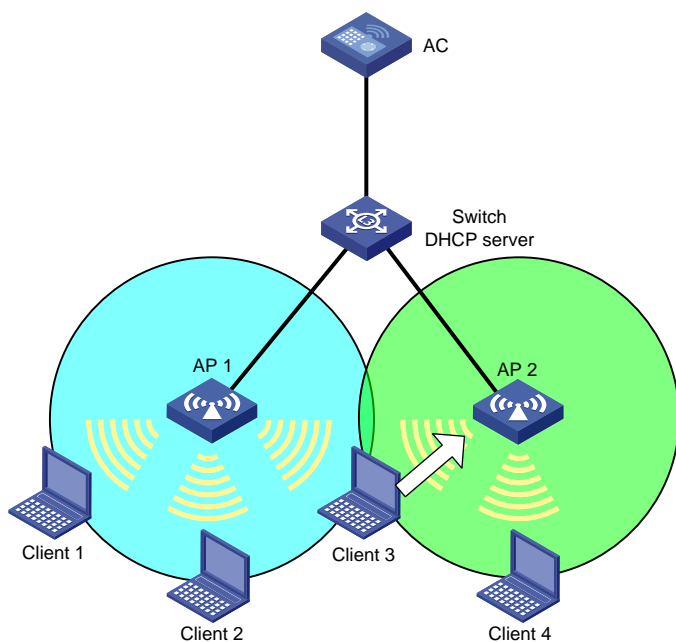
本文档假设您已了解 WLAN RRM 特性。

## 3 会话模式的负载均衡配置举例

### 3.1 组网需求

如图 1 所示，无线网络中 AC 下关联两台 AP，三层交换机 Switch 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址。要求 AP 之间根据客户端数量进行负载分担，当 AP 关联的客户端数量达到 3 个，且 AP 之间关联的无线客户端数量差值达到 2 个时，如果需要上线的客户端处在 AP 1 和 AP 2 的信号重叠区，则 AP 启动负载均衡。

图1 会话模式的负载均衡组网图



## 3.2 配置思路

为避免 AP 负载均衡拒绝客户端关联请求次数过多，使客户端上线时间过长，需要配置 AP 拒绝客户端关联请求的最大次数。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应,AP 的序列号可以通过 AP 设备背面的标签获取。
- 每个 AP 上必须绑定相同的服务模板，并且保证各个 radio 开启的模式是一样的。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.100.1 255.255.255.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，IP 地址为 192.168.200.1/24。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.168.200.1 255.255.255.0
[AC-Vlan-interface200] quit
```

#### (2) 配置负载均衡

# 配置 GigabitEthernet1/0/1 接口的链路类型为 Hybrid，允许 VLAN 100 和 VLAN 200 的报文通过，并且发送这些 VLAN 的报文时携带 VLAN Tag。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type hybrid
[AC-GigabitEthernet1/0/1] port hybrid vlan 100 200 tagged
[AC-GigabitEthernet1/0/1] quit
```

# 进入 RRM 视图。

```
[AC] wlan rrm
```

# 配置会话门限值为 3，会话差值门限为 2，当 AP 之间客户端差值为 2 以上时，认为处于不平衡状态。

```
[AC-wlan-rrm] load-balance session 3 gap 2
```

# 配置 AP 拒绝客户端关联请求的最大次数为 4。

```
[AC-wlan-rrm] load-balance access-denial 4
```

```

[AC-wlan-rrm] quit
(3) 在 AC 上配置 AP 并绑定无线服务
# 创建 WLAN-ESS 接口 1，并配置 WLAN-ESS 1 接口加入 VLAN 200。
[AC] interface WLAN-ESS 1
[AC-WLAN-ESS1] port access vlan 200
[AC-WLAN-ESS1] quit
# 创建 clear 类型的服务模板 1。
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS 1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 使能无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
# 创建 AP 管理模板，其名称为 ap1，型号名称这里选择 WA2620E-AGN。
[AC] wlan ap ap1 model WA2620E-AGN
# 配置 AP 1 的序列号为 21023529G007C000020。
[AC-wlan-ap-ap1] serial-id 21023529G007C000020
# 设置 radio 2 的射频类型为 802.11gn。
[AC-wlan-ap-ap1] radio 2 type dot11gn
# 将服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-ap1-radio-2] service-template 1
# 配置射频的工作信道为 6。
[AC-wlan-ap-ap1-radio-2] channel 6
# 使能 AP 1 的 radio2。
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
# 创建 AP 管理模板，其名称为 ap2，型号名称这里选择 WA2620E-AGN。
[AC] wlan ap ap2 model WA2620E-AGN
# 配置 AP 2 的序列号为 21023529G007C000021。
[AC-wlan-ap-ap2] serial-id 21023529G007C000021
# 设置 radio2 的射频类型为 802.11gn。
[AC-wlan-ap-ap2] radio 2 type dot11gn
# 将服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-ap2-radio-2] service-template 1
# 配置射频的工作信道为 6。
[AC-wlan-ap-ap2-radio-2] channel 6
# 使能 AP 2 的 radio2。
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] return

```



### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200,其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量,VLAN 200 为无线用户接入的 VLAN。

```
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口链路类型为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口链路类型为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 使能 DHCP 服务。

```
[Switch] dhcp enable
```

# 创建名为 vlan100 的 DHCP 地址池, 配置动态分配的网段为 192.168.100.0/24, 网关地址为 192.168.100.1, 为 AP 1 和 AP 2 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.168.100.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan100] gateway-list 192.168.100.1
[Switch-dhcp-pool-vlan100] quit
```

# 创建名为 vlan200 的 DHCP 地址池, 配置动态分配的网段为 192.168.200.0/24, 网关地址为 192.168.200.1, 为 Client 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.168.200.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan200] gateway-list 192.168.200.1
[Switch-dhcp-pool-vlan200] quit
```

## 3.5 验证配置

- (1) AP 1 关联了 3 个用户, 由于 AC 配置了会话模式的负载均衡, 当 AP 1 的会话数达到门限值 3, 且比 AP 2 的会话数多 2 个时, 就是触发负载均衡。
- (2) 当 Client 3 发现并试图关联到 AP 1 时, 可以看到 AP 1 上的会话数已经达到门限值 3, 并比 AP 2 多了 2 个, 所以 AP 1 会拒绝 Client 3 的接入, 最终 Client 3 会关联到 AP 2 上。

## 3.6 配置文件

- AC:

```
#
vlan 100
#
vlan 200
#
wlan rrm
    load-balance session 3 gap 2
    load-balance access-denial 4
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
interface Vlan-interface100
    ip address 192.168.100.1 255.255.255.0
#
interface Vlan-interface200
    ip address 192.168.200.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type hybrid
    port hybrid vlan 100 200 tagged
#
interface WLAN-ESS1
    port access vlan 200
#
wlan ap ap1 model WA2620E-AGN
    serial-id 21023529G007C000020
    radio 2 type dot11gn
        channel 6
        service-template 1
    radio enable
#
wlan ap ap2 model WA2620E-AGN
    serial-id 21023529G007C000021
    radio 2 type dot11gn
```

```

channel 6
service-template 1
radio enable
#
• Switch:
#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
network 192.168.100.0 mask 255.255.255.0
gateway-list 192.168.100.1
#
dhcp server ip-pool vlan200
network 192.168.200.0 mask 255.255.255.0
gateway-list 192.168.200.1
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
poe enable
#

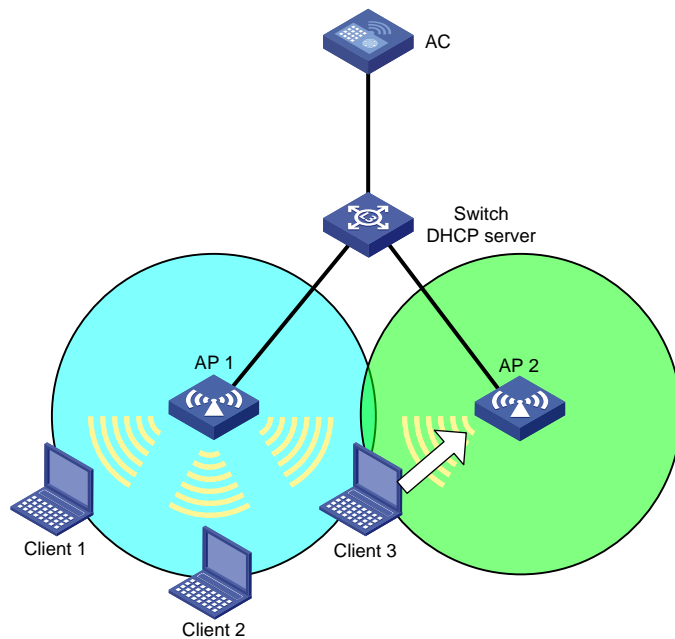
```

## 4 流量模式的负载均衡配置举例

### 4.1 组网需求

如图 2 所示,无线网络中 AC 下关联两台 AP,三层交换机 Switch 作为 DHCP Server 为 AP 和 Client 分配 IP 地址。要求 AP 之间根据流量进行负载分担,设置 AP 最大带宽为 30M,当通过 AP 的流量占用 AP 最大带宽的 50%,且 AP 之间的流量占用带宽的差值达到 AP 最大带宽的 30%时,如果需要上线的客户端处在 AP 1 和 AP 2 的信号重叠区,则 AP 启动负载均衡。

图2 流量模式的负载均衡组网图



## 4.2 配置思路

为避免 AP 负载均衡拒绝客户端关联请求次数过多，使客户端上线时间过长，需要配置 AP 拒绝客户端关联请求的最大次数。

## 4.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应,AP 的序列号可以通过 AP 设备背面的标签获取。
- 每个 AP 上必须绑定相同的服务模板，并且保证各个 radio 开启的模式是一样的。

## 4.4 配置步骤

### 4.4.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.100.1 255.255.255.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，IP 地址为 192.168.200.1/24。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.168.200.1 255.255.255.0
[AC-Vlan-interface200] quit
```

## (2) 配置负载均衡

# 配置 GigabitEthernet1/0/1 接口的链路类型为 Hybrid，允许 VLAN 100 和 VLAN 200 的报文通过，并且发送这些 VLAN 的报文时保留 VLAN Tag。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type hybrid
[AC-GigabitEthernet1/0/1] port hybrid vlan 100 200 tagged
[AC-GigabitEthernet1/0/1] quit
```

# 进入 RRM 视图。

```
[AC] wlan rrm
```

# 配置最大带宽为 30M。

```
[AC-wlan-rrm] dot11n max-bandwidth 30000
```

# 配置流量门限值为 50%，流量差值门限为 30%。

```
[AC-wlan-rrm] load-balance traffic 50 gap 30
```

# 配置 AP 拒绝客户端关联请求的最大次数为 4

```
[AC-wlan-rrm] load-balance access-denial 4
```

# 创建 WLAN-ESS 接口 1，并配置 WLAN-ESS 1 接口加入 VLAN 200。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port access vlan 200
[AC-WLAN-ESS1] quit
```

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 使能无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

## (3) 在 AC 上配置 AP 并绑定无线服务

# 创建 AP 管理模板，其名称为 ap1，型号名称这里选择 WA2620E-AGN。

```
[AC] wlan ap ap1 model WA2620E-AGN
```

# 配置 AP 1 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-ap1] serial-id 21023529G007C000020
```

# 设置 radio 2 的射频类型为 802.11gn。

```
[AC-wlan-ap-ap1] radio 2 type dot11gn
```

# 将服务模板 1 与射频 2 进行关联。

```
[AC-wlan-ap-ap1-radio-2] service-template 1
```

```

# 配置射频的工作信道为 6。
[AC-wlan-ap-ap1-radio-2] channel 6
# 使能 AP 1 的 radio 2。
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
# 创建 AP 管理模板，其名称为 ap2，型号名称这里选择 WA2620E-AGN。
[AC] wlan ap ap2 model WA2620E-AGN
# 配置 AP 2 的序列号为 21023529G007C000021。
[AC-wlan-ap-ap2] serial-id 21023529G007C000021
# 设置 radio 2 的射频类型为 802.11gn。
[AC-wlan-ap-ap2] radio 2 type dot11gn
# 将服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-ap2-radio-2] service-template 1
# 配置射频的工作信道为 6。
[AC-wlan-ap-ap2-radio-2] channel 6
# 使能 AP 2 的 radio 2。
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] return

```

#### 4.4.2 Switch 的配置

```

# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 200 为无线用户接入的 VLAN。
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 200 通过。
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口链路类型为 Access，当前 Access 口允许 VLAN 100 通过。
[Switch] interface GigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口链路类型为 Access，当前 Access 口允许 VLAN 100 通过。
[Switch] interface GigabitEthernet1/0/3

```

```
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
# 配置 Switch 使能 DHCP 服务。
[Switch] dhcp enable
# 创建名为 vlan100 的 DHCP 地址池，配置动态分配的网段为 192.168.100.0/24，网关地址为 192.168.100.1，为 AP 1 和 AP 2 分配 IP 地址。
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.168.100.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan100] gateway-list 192.168.100.1
[Switch-dhcp-pool-vlan100] quit
# 创建名为 vlan200 的 DHCP 地址池，配置动态分配的网段为 192.168.200.0/24，网关地址为 192.168.200.1，为 Client 分配 IP 地址。
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.168.200.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan200] gateway-list 192.168.200.1
[Switch-dhcp-pool-vlan200] quit
```

## 4.5 验证配置

- (1) 由于 AC 上配置了流量负载均衡，当 AP 的最大带宽为 30M 时，系统的流量门限为  $30M \times 50\% = 15M$ ，流量差值门限为  $30M \times 30\% = 9M$ 。
- (2) 当 Client 1 和 Client 2 关联到 AP 1 时，使用发送流量的工具 IxChariot 给 AP 1 打流量，让 AP 1 上此时的流量大于 17M。
- (3) 此时 AP 2 上由于没有无线用户关联，所以没有流量。
- (4) 当 Client 3 发现并试图关联到 AP 1 时，由于 AC 上启用了流量负载均衡功能，此时 AP 1 上的流量为 17M（大于 AC 上配置的流量门限 15M 和流量差值门限 9M），所以 AC 会拒绝 Client 3 对 AP 1 的关联请求，Client 3 只能关联到 AP 2 上。

## 4.6 配置文件

- AC:
 

```
#
vlan 100
#
vlan 200
#
wlan rrm
dot11n max-bandwidth 30000
load-balance traffic 50 gap 30
load-balance access-denial 4
#
wlan service-template 1 clear
ssid service
```

```

bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 192.168.100.1 255.255.255.0
#
interface Vlan-interface200
ip address 192.168.200.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 100 200 tagged
#
interface WLAN-ESS1
port access vlan 200
#
wlan ap ap1 model WA2620E-AGN
serial-id 21023529G007C000020
radio 2 type dot11gn
channel 6
service-template 1
radio enable
#
wlan ap ap2 model WA2620E-AGN
serial-id 21023529G007C000021
radio 2 type dot11gn
channel 6
service-template 1
radio enable

```

#### ● Switch:

```

#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
network 192.168.100.0 mask 255.255.255.0
gateway-list 192.168.100.1
#
dhcp server ip-pool vlan200
network 192.168.200.0 mask 255.255.255.0
gateway-list 192.168.200.1
#
interface GigabitEthernet1/0/1
port link-type trunk

```



```
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
poe enable
#
```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 禁止弱信号无线客户端接入典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                       |   |
|-----------------------|---|
| 1 简介.....             | 1 |
| 2 配置前提 .....          | 1 |
| 3 配置举例 .....          | 1 |
| 3.1 组网需求 .....        | 1 |
| 3.2 配置注意事项.....       | 1 |
| 3.3 配置步骤.....         | 2 |
| 3.3.1 AC 配置.....      | 2 |
| 3.3.2 Switch 配置 ..... | 4 |
| 3.4 验证配置 .....        | 5 |
| 3.5 配置文件.....         | 6 |
| 4 相关资料 .....          | 8 |

# 1 简介

本文档介绍了在 AC 设备上禁止弱信号无线客户端接入功能的典型配置案例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解禁止弱信号客户端接入功能的特性。

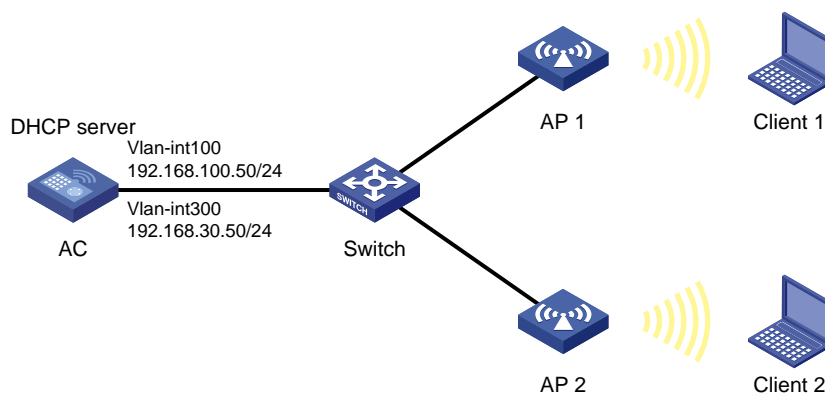
## 3 配置举例

### 3.1 组网需求

如图 1 所示，Client 访问无线网络，AC 通过 Switch 连接 AP 1 和 AP 2，AC 充当 DHCP 服务器为 AP 和 Client 分配 IP 地址，Client 1 和 Client 2 分别连接到 AP 1 和 AP 2。现要求：

- 对于信号强度大于等于 15dBm 的无线客户端，允许其接入并且正常为其分配地址，可以访问指定网络内的资源。
- 对于信号强度小于 15dBm 的无线客户端，禁止其接入到无线网络中，该无线客户端无法访问网络资源。

图1 禁止弱信号无线客户端接入组网图



### 3.2 配置注意事项

- 无线客户端成功连接到无线网络后，即使移动到 AP 信号强度较弱的地方，链路也不会被无线控制器主动断开。如果无线客户端主动断开连接后，该策略将会对新的接入过程生效。

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应, AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 配置

#### (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口, 并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.100.50 255.255.255.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN, 配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 192.168.30.50 255.255.255.0
[AC-Vlan-interface300] quit
```

# 配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型, 禁止 VLAN 1 报文通过, 允许 VLAN 100 和 VLAN 300 通过, 当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 DHCP 服务

# 使能 DHCP 服务。

```
[AC] dhcp enable
```

# 创建名为 vlan100 的 DHCP 地址池, 为 AP 分配网段为 192.168.100.0/24, 网关地址为 192.168.100.50。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 192.168.100.0 mask 255.255.255.0
[AC-dhcp-pool-vlan100] gateway-list 192.168.100.50
[AC-dhcp-pool-vlan100] quit
```

# 创建名为 vlan300 的 DHCP 地址池, 为 Client 分配网段为 192.168.30.0/24, 网关地址为 192.168.30.50。

```
[AC] dhcp server ip-pool vlan300
```

```
[AC-dhcp-pool-vlan300] network 192.168.30.0 mask 255.255.255.0
[AC-dhcp-pool-vlan300] gateway-list 192.168.30.50
[AC-dhcp-pool-vlan300] quit
```

### (3) 配置 WLAN-ESS 接口

# 创建 WLAN-ESS 1 接口，并进入该视图。

```
[AC] interface wlan-ess 1
```

# 配置接口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置接口 WLAN-ESS1 的缺省 VLAN 为 VLAN 200，禁止 VLAN 1 报文通过，并允许发送 VLAN 200 报文不带 VLAN tag。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

### (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID（服务模板的标识）为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 开启服务模板 1。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

### (5) 配置射频接口并绑定服务模板

# 创建 AP 管理模板 ap1，型号名称选择 WA2620E-AGN，并配置序列号 21023529G007C000020。

```
[AC] wlan ap ap1 model WA2620E-AGN
```

```
[AC-wlan-ap-ap1] serial-id 21023529G007C000020
```

# 进入 AP 的射频视图。

```
[AC-wlan-ap-ap1] radio 2
```

# 将配置的服务模板 1 映射到 radio 2，并设置绑定到射频接口的 VLAN 编号为 VLAN 300。

```
[AC-wlan-ap-ap1-radio-2] service-template 1 vlan-id 300
```

# 开启 AP 1 的 radio 2。

```
[AC-wlan-ap-ap1-radio-2] radio enable
```

```
[AC-wlan-ap-ap1-radio-2] quit
```

```
[AC-wlan-ap-ap1] quit
```

# 创建 AP 管理模板 ap2，型号名称选择 WA2620E-AGN，并配置序列号 21023529G007C000021。

```
[AC] wlan ap ap2 model WA2620E-AGN
```

```
[AC-wlan-ap-ap2] serial-id 21023529G007C000021
```

# 进入 AP 的射频视图。

```
[AC-wlan-ap-ap2] radio 2
```

# 将配置的服务模板 1 映射到 radio 2，并设置绑定到射频接口的 VLAN 编号为 VLAN 300。

```
[AC-wlan-ap-ap2-radio-2] service-template 1 vlan-id 300
```

# 开启 AP 1 的 radio 2。

```
[AC-wlan-ap-ap2-radio-2] radio enable
```

```
[AC-wlan-ap-ap2-radio-2] quit
```

```
[AC-wlan-ap-ap2] quit
```

(6) 启用禁止弱信号无线客户端接入策略。

# 禁止信号强度低于 15dbm 的无线客户端接入。

```
[AC] wlan option client-reject 15
```

### 3.3.2 Switch 配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 配置 Switch 和 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk, 禁止 VLAN 1 报文通过, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Access, 当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
```

```
[Switch-GigabitEthernet1/0/3] port link-type access
```

```
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/3] poe enable
```

```
[Switch-GigabitEthernet1/0/3] quit
```

## 3.4 验证配置

# 在启用禁止弱信号接入应用策略前，通过命令 **display wlan client verbose** 可以观察到弱信号的无线客户端（RSSI 为 10）。

```
<AC> display wlan client verbose
Total Number of Clients : 1
Client Information
-----
MAC Address : 001e-claa-f5bd
User Name   : -NA-
AID : 1
AP Name : ap1
Radio Id : 2
SSID : service
BSSID : 0023-8993-7550
Port : WLAN-DBSS1:1
VLAN : 300
State : Running
Power Save Mode : Active
Wireless Mode : 11gn
QoS Mode : WMM
Listen Interval (Beacon Interval) : 10
RSSI : 10
Rx/Tx Rate : 48/36
Client Type : PRE-RSNA
Authentication Method : Open System
AKM Method : None
4-Way Handshake State : -NA-
Group Key State : -NA-
Encryption Cipher : Clear
Roam Status : Normal
Roam Count : 0
Up Time (hh:mm:ss) : 00:09:34
```

# 启用禁止弱信号接入应用策略后，通过命令 **display wlan client verbose** 观察到无线客户端不会断开连接。

```
<AC> display wlan client verbose
Total Number of Clients : 1
Client Information
-----
MAC Address : 001e-claa-f5bd
User Name   : -NA-
AID : 1
AP Name : ap1
Radio Id : 2
SSID : service
BSSID : 0023-8993-7550
Port : WLAN-DBSS1:1
```



```

VLAN : 300
State : Running
Power Save Mode : Active
Wireless Mode : 11gn
QoS Mode : WMM
Listen Interval (Beacon Interval) : 10
RSSI : 10
Rx/Tx Rate : 48/36
Client Type : PRE-RSNA
Authentication Method : Open System
AKM Method : None
4-Way Handshake State : -NA-
Group Key State : -NA-
Encryption Cipher : Clear
Roam Status : Normal
Roam Count : 0
Up Time (hh:mm:ss) : 00:12:10

```

# 断开无线客户端连接,再使无线客户端重新和AP建立连接。此时,该无线客户端无法接入到WLAN网络,通过命令 **display wlan client verbose** 查看不到无线客户端信息。

## 3.5 配置文件

```

• AC:

#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
network 192.168.100.0 mask 255.255.255.0
gateway-list 192.168.100.50
#
dhcp server ip-pool vlan300
network 192.168.30.0 mask 255.255.255.0
gateway-list 192.168.30.50
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 192.168.100.50 255.255.255.0
#
interface Vlan-interface300
ip address 192.168.30.50 255.255.255.0

```

```

#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 300
 undo port trunk permit vlan 1
 port trunk pvid vlan 100
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
 serial-id 21023529G007C000020
 radio 2
 service-template 1 vlan-id 300
 radio enable
#
wlan ap ap2 model WA2620E-AGN id 1
 serial-id 21023529G007C000021
 radio 2
 service-template 1 vlan-id 300
 radio enable
#
 wlan option client-reject 15
#
dhcp enable
#
•   Switch:
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 300
 undo port trunk permit vlan 1
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
#
interface GigabitEthernet1/0/3

```

```
port link-type access
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 空口队列智能带宽保障典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤 .....         | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 3 |
| 3.4 验证配置 .....         | 4 |
| 3.5 配置文件 .....         | 5 |
| 4 相关资料 .....           | 7 |

# 1 简介

本文介绍了通过配置相应业务的传输带宽来保障语音和视频的可靠传输的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

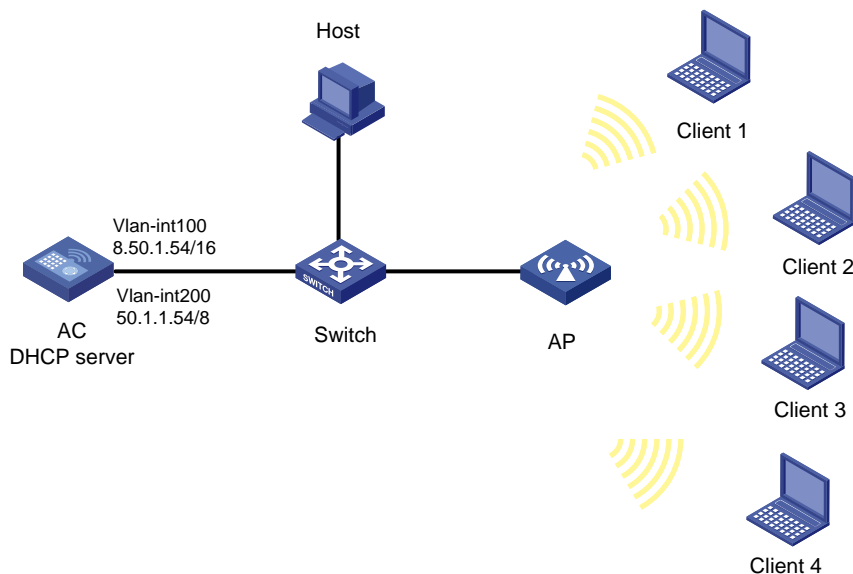
本文档假设您已了解 WLAN QoS 的相关功能。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 作为 DHCP Server 为 AP 和 Client 分配 IP 地址，无线客户端通过 AP 接入无线网络，Host 主机分别向四台客户端传输数据，利用 Chariot 软件设置对应的优先级分别为 VO/VI/BE/BK。现要求：开启智能带宽保障的功能，优先保证 VO 队列的流量为 20Mbps，VI 队列的流量为 10Mbps。

图1 智能带宽保障组网图



### 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 8.50.1.54 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN 和 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 50.1.1.54 8
[AC-Vlan-interface200] quit
```

# 配置 AC 与 Switch 相连的接口的 GigabitEthernet1/0/1 接口的链路类型为 Trunk 类型，当前 Trunk 口的 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 和 Client 使用的 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 DHCP 服务

# 使能 DHCP 服务

```
<AC> system-view
[AC] dhcp enable
```

# 在 AC 上配置 AP 注册使用的地址池 ap，分配地址为 8.50.0.0/16 网段的地址，网关地址为 8.50.1.54。

```
[AC] dhcp server ip-pool ap
[AC-dhcp-pool-ap] network 8.50.0.0 16
[AC-dhcp-pool-ap] gateway-list 8.50.1.54
[AC-dhcp-pool-ap] quit
```

# 在 AC 上配置 Client 使用的地址池 client，分配地址为 50.0.0.0/8 网段的地址，网关地址为 50.1.1.54。

```
[AC] dhcp server ip-pool client
[AC-dhcp-pool-client] network 50.0.0.0 8
[AC-dhcp-pool-client] gateway-list 50.1.1.54
[AC-dhcp-pool-client] quit
```

# 创建 WLAN-ESS0 口，配置 WLAN-ESS0 接口类型为 Hybrid 类型。

```
[AC] interface wlan-ess 0
```

```
[AC-WLAN-ESS0] port link-type hybrid
# 配置 WLAN-ESS0 口的 PVID 为 VLAN 200, 允许 VLAN 200 不带 tag 通过。
```

```
[AC-WLAN-ESS0] port hybrid vlan 200 untagged
[AC-WLAN-ESS0] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS0] mac-vlan enable
[AC-WLAN-ESS0] quit
```

### (3) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS0 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 0
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### (4) 配置 AP

# 创建 AP 的管理模板, 名称为 officeap, 型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 AP 的 radio 射频视图, 将服务模板 1 绑定到 AP 的 radio2 后使能射频。

```
[AC-wlan-ap-officeap] radio 2
[AC-wlan-ap-officeap-radio-2] service-template 1
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

### (5) 配置智能带宽保障

# 开启基于队列调度的智能带宽保障功能, 配置射频接口进行带宽保障, 配置总带宽为 40Mbps, 保障 VO 语音队列 20Mbps 和 VI 视频队列 10Mbps。

```
[AC] wlan option bandwidth-guarantee vo 20 vi 10 total 40 iphead
```

## 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk, 配置 PVID 为 200, 允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet1/0/1
```



```
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 200
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 Host 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

### 3.4 验证配置

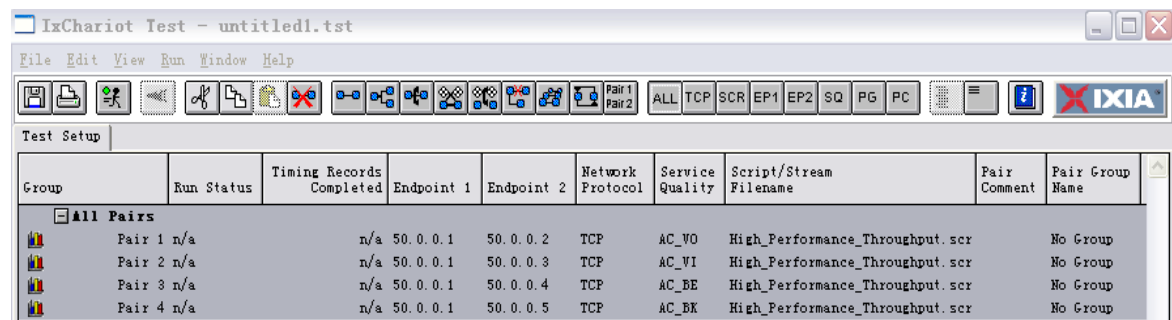
(1) 配置完成后，在 AC 上通过命令行 **display wlan client** 查看四个 Client 全部通过业务 VLAN 上线，而且正常获得 IP 地址。

```
[AC] display wlan client
Total Number of Clients          : 4
Client Information
SSID: service
```

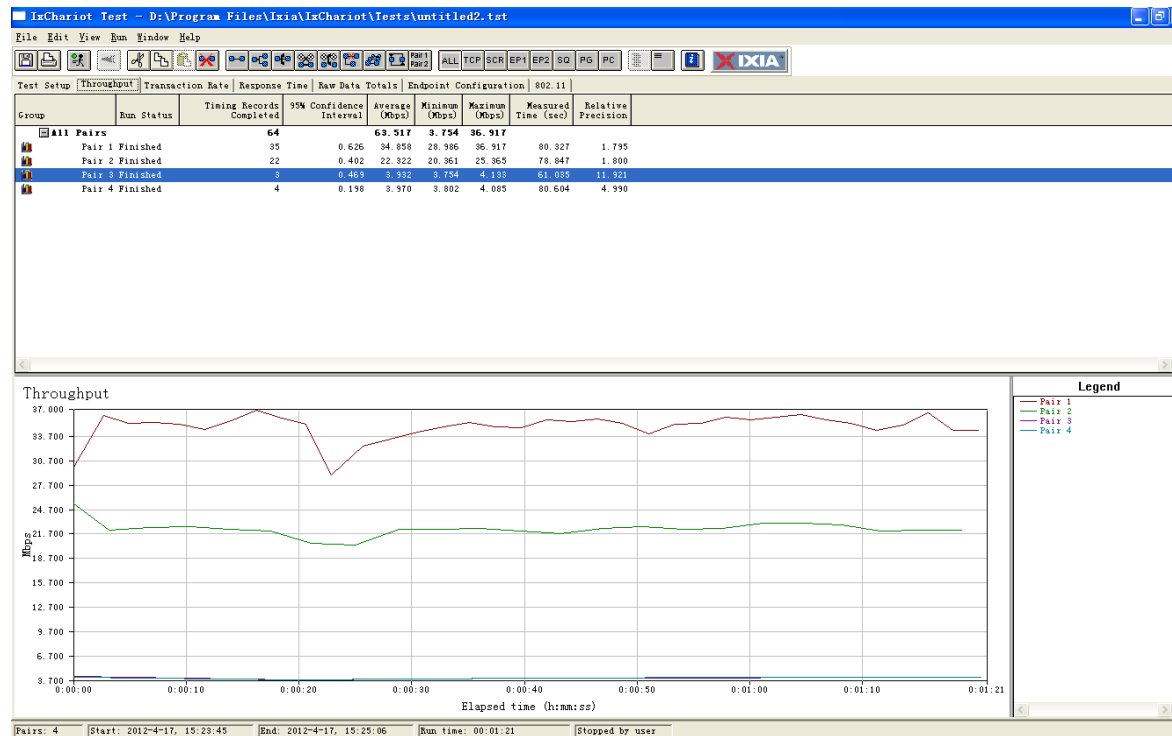
| MAC Address    | User Name | APID/RID | IP Address | VLAN |
|----------------|-----------|----------|------------|------|
| 0015-005c-92f4 | -NA-      | 1 /2     | 50.0.0.2   | 200  |
| 0021-63a4-3be4 | -NA-      | 1 /2     | 50.0.0.3   | 200  |
| 0024-0130-6904 | -NA-      | 1 /2     | 50.0.0.4   | 200  |
| 0021-2708-b41f | -NA-      | 1 /2     | 50.0.0.5   | 200  |

[AC]

(2) 在 Host 上运行 Chariot 软件。使用 Chariot 软件构造流量。从有线打向无线，每个 Client 构造一条流量，构造流量优先级分别为 VO、VI、BE、BK，如下图所示：



- (3) 运行 Chariot 软件，会有如下的测试结果。其中下图中位于上面的红色曲线和绿色曲线分别代表着 VO 队列和 VI 队列的性能曲线；位于下面的两条曲线分别代表着 BE 队列和 BK 队列的性能曲线。



## 3.5 配置文件

```

• AC
#
vlan 100
#
vlan 200
#
dhcp server ip-pool ap
network 8.50.0.0 mask 255.255.0.0
gateway-list 8.50.1.54
#
dhcp server ip-pool client
network 50.0.0.0 mask 255.0.0.0
gateway-list 50.1.1.54
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 0
service-template enable
#
interface Vlan-interface100

```

```

ip address 8.50.1.54 255.255.0.0
#
interface Vlan-interface200
ip address 50.1.1.54 255.0.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk permit vlan 100 200
#
interface WLAN-ESS0
port link-type hybrid
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1
radio enable
#
wlan option bandwidth-guarantee vo 20 vi 10 total 40 iphead
#

```

## - Switch

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 来宾用户访问管理 Portal 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤.....          | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 4 |
| 3.4 验证配置 .....         | 4 |
| 3.5 配置文件.....          | 6 |
| 4 相关资料 .....           | 7 |

# 1 简介

本文档介绍来宾用户访问管理 Portal 典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

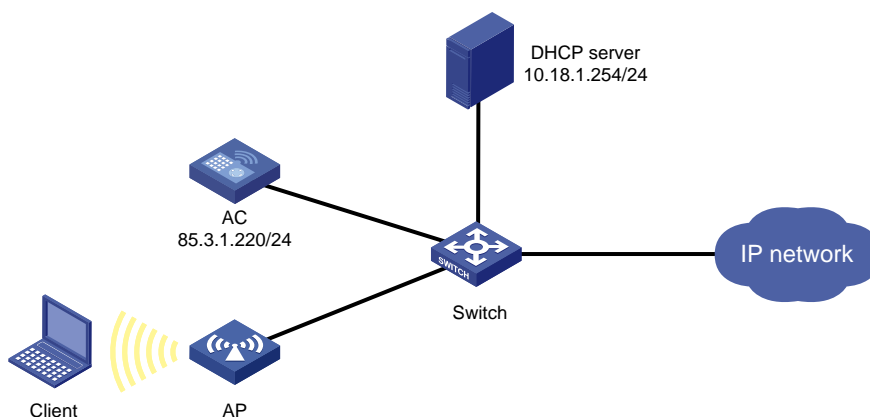
本文档假设您已了解 Portal 特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，局域网内用户 Client 通过无线网络访问外部网络，Client 和 AP 通过 DHCP 服务器获取 IP 地址。AC 与 AP 通过二层交换机相连，配置 AC 采用本地 Portal 方式认证来访的来宾用户，并通过 ACL 对来宾用户的访问权限进行控制。

图1 来宾用户访问管理 Portal 组网图



### 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 10 及其对应的 VLAN 接口，并为该接口配置 IP 地址。使用该接口的 IP 地址与 AP 建立 LWAPP 隧道，同时作为 Client 接入的业务 VLAN。

```
<AC> system-view
[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 85.3.1.220 255.255.255.0
```

# 配置 AC 1 与 Switch 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk, PVID 为 10, 允许 VLAN 10 的报文通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 10
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 10
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS 接口 2，并将 WLAN-ESS 2 接口加入 VLAN 10 中。

```
[AC] interface wlan-ess 2
[AC-WLAN-ESS2] port access vlan 10
[AC-WLAN-ESS2] quit
```

#### (2) 配置 Portal 认证

# 配置 Portal 服务器 local 的 IP 地址为 85.3.1.220、HTTP 重定向的 URL 为 http://85.3.1.220/portal/logon.htm。

```
[AC] portal server local ip 85.3.1.220 url http://85.3.1.220/portal/logon.htm
```

# 配置本地 Portal 服务器支持 HTTP 协议方式。

```
[AC] portal local-server http
```

# 进入 ISP 域 system。

```
[AC] domain system
```

# 为 Portal 用户配置认证方法和授权方法分别为 local。

```
[AC-isp-system] authentication portal local
[AC-isp-system] authorization portal local
[AC-isp-system] quit
```

# 指定 Portal 服务器 local，并配置为直接认证方式。

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] portal server local method direct
```

# 指定从 VLAN 10 接口上接入的 IPv4 Portal 用户使用认证域 system。

```
[AC-Vlan-interface10] portal domain system
[AC-Vlan-interface10] quit
```

#### (3) 配置服务模板

# 配置 WLAN 服务模板 3，并使用明文方式发送数据。

```
[AC] wlan service-template 3 clear
```



# 配置 SSID 为 portal，并将 WLAN-ESS 接口 2 与该服务模板绑定。

```
[AC-wlan-st-3] ssid portal
[AC-wlan-st-3] bind wlan-ess 2
```

# 启动无线服务。

```
[AC-wlan-st-3] service-template enable
[AC-wlan-st-3] quit
```

#### (4) 配置 AP

# 创建 AP 的管理模板，名称为 ap22，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap ap22 model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-ap22] serial-id 21023529G007C000020
```

# 进入 AP 的 radio 2 射频视图。

```
[AC-wlan-ap-ap22] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 3 与射频 2 进行关联。

```
[AC-wlan-ap-ap22-radio-2] service-template 3
```

# 使能 AP 的 radio 2。

```
[AC-wlan-ap-ap22-radio-2] radio enable
[AC-wlan-ap-ap22-radio-2] quit
[AC-wlan-ap-ap22] quit
```

#### (5) 配置 ACL 和来宾用户信息

# 配置 ACL，为便于验证，本文仅允许访问目的 IP 地址为 8.1.1.16 和 8.1.1.20 的报文，拒绝其他的 IP 报文。

```
[AC] acl number 3322
[AC-acl-adv-3322] rule 0 permit ip destination 8.1.1.16 0
[AC-acl-adv-3322] rule 5 permit ip destination 8.1.1.20 0
[AC-acl-adv-3322] rule 10 deny ip
```

# 添加本地用户 guest，设置来宾用户密码为 guest、服务类型为 portal、过期时间为 2014 年 1 月 31 日 18 点、用户角色为 guest、授权 ACL 为 3322。

```
[AC] local-user guest
```

# 设置用户密码为 guest。

```
[AC-luser-guest] password simple guest
```

# 设置服务类型为 portal。

```
[AC-luser-guest] service-type portal
```

# 设置用户 guest 的有效期为 2014 年 1 月 31 日 18 点。

```
[AC-luser-guest] expiration-date 18:00:00-2014/1/31
```

# 授权本地用户为来宾用户。

```
[AC-luser-guest] authorization-attribute user-role guest
```

# 设置本地用户 guest 的授权 ACL 的编号为 3322，本地用户 guest 认证成功后，将被授权可以访问符合 ACL 3322 规则的网络资源。

```
[AC-luser-guest] authorization-attribute acl 3322
[AC-luser-guest] return
```

### 3.3.2 Switch 的配置

# 创建 VLAN 10, 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, 且做为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性为 Trunk, PVID 为 10, 允许 VLAN 10 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 10
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 10
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 10 通过, 并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 10
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口属性为 Access, 并允许 VLAN 10 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 10
[Switch-GigabitEthernet1/0/3] quit
```

### 3.4 验证配置

(1) 使用命令行 **display portal user all** 查看是否有用户在线。

```
<AC> display portal user all
Index:1919
State:ONLINE
SubState:NONE
ACL:3322
Work-mode:stand-alone
MAC                IP                Vlan    Interface
-----
001e-c144-472e     85.3.1.100        10      Vlan-interface10
Total 1 user(s) matched, 1 listed.
```

(2) 通过命令行 **display connection ucibindex** 查看来宾用户连接的详细信息。

```
<AC> display connection ucibindex 1919
Index=1919, Username=guest@system
MAC=00-1E-C1-44-47-2E
IP=85.3.1.100
IPv6=N/A
Access=PORTAL ,AuthMethod=PAP
```

Port Type=Wireless-802.11,Port Name=Vlan-interface10  
Initial VLAN=10, Authorization VLAN=10  
ACL Group=3322  
User Profile=N/A  
CAR=Disable  
Priority=Disable  
Start=2014-01-30 10:20:03 ,Current=2014-01-30 10:27:19 ,Online=00h07m16s  
Total 1 connection matched.

- (3) 通过 **ping** 命令可以验证来宾用户的访问权限，可以看到来宾用户只能访问被授权的地址，其他地址不允许访问。

D:\> ping 8.1.1.16

Pinging 8.1.1.16 with 32 bytes of data:

Reply from 8.1.1.16: bytes=32 time=19ms TTL=254  
Reply from 8.1.1.16: bytes=32 time<1ms TTL=254  
Reply from 8.1.1.16: bytes=32 time<1ms TTL=254  
Reply from 8.1.1.16: bytes=32 time<1ms TTL=254

Ping statistics for 8.1.1.16:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) ,  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 19ms, Average = 4ms

D:\> ping 8.1.1.20

Pinging 8.1.1.20 with 32 bytes of data:

Reply from 8.1.1.20: bytes=32 time=19ms TTL=254  
Reply from 8.1.1.20: bytes=32 time<1ms TTL=254  
Reply from 8.1.1.20: bytes=32 time<1ms TTL=254  
Reply from 8.1.1.20: bytes=32 time<1ms TTL=254

Ping statistics for 8.1.1.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) ,  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 19ms, Average = 4ms

D:\> ping 8.1.1.22

Pinging 8.1.1.22 with 32 bytes of data:

Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.

Ping statistics for 8.1.1.22:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

## 3.5 配置文件

- AC 的配置文件:

```
#
port-security enable
#
portal server local ip 85.3.1.220 url http://85.3.1.220/portal/logon.htm
portal local-server http
#
acl number 3322
rule 0 permit ip destination 8.1.1.16 0
rule 5 permit ip destination 8.1.1.20 0
rule 10 deny ip
#
vlan 10
#
domain system
authentication portal local
authorization portal local
access-limit disable
state active
idle-cut disable
self-service-url disable
#
user-group system
group-attribute allow-guest
#
local-user guest
password simple guest
authorization-attribute acl 3322
authorization-attribute user-role guest
service-type portal
expiration-date 18:00:00-2014/01/31
#
wlan service-template 3 clear
ssid portal
bind WLAN-ESS 2
service-template enable
#
interface Vlan-interface10
ip address 85.3.1.220 255.255.255.0
portal server local method direct
portal domain system
#
interface WLAN-ESS2
port access vlan 10
```

```
#
wlan ap 22 model WA2620E-AGN
serial-id 21023529G007C000020
radio 2
channel 1
service-template 3
radio enable
```

```
#
```

- Switch 的配置文件:

```
#
```

```
vlan 100
```

```
#
```

```
vlan 300
```

```
#
```

```
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100
port trunk pvid vlan 100
```

```
#
```

```
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 100
port trunk pvid vlan 100
```

```
#
```

```
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
```

```
#
```

```
interface GigabitEthernet1/0/4
port link-type access
port access vlan 100
poe enable
```

```
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“ACL 和 QoS 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“ACL 和 QoS 命令参考”。

# 明文无线接入服务典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤.....          | 1 |
| 3.3.1 AC 的配置 .....     | 1 |
| 3.3.2 Switch 的配置 ..... | 3 |
| 3.4 验证配置 .....         | 4 |
| 3.5 配置文件 .....         | 5 |
| 4 相关资料 .....           | 7 |

# 1 简介

本文介绍了明文无线接入服务典型配置案例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

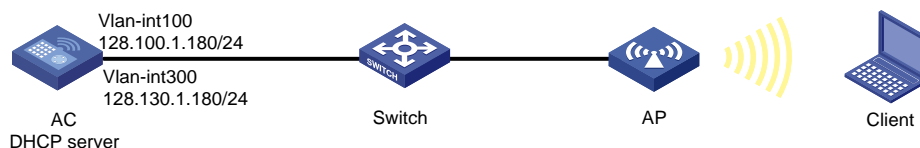
本文档假设您已了解 WLAN 无线接入和 WLAN 安全特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AP 通过交换机与 AC 相连，AC 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址，现要求：通过配置开放式系统认证方式实现无线终端用户可以不需要输入用户名和密码即可接入 WLAN 网络的目的。

图1 明文方式接入无线服务配置组网图



### 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.3 配置步骤

#### 3.3.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
```



# 配置 VLAN 100 的接口 IP 地址为 128.100.1.180/24。

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 128.100.1.180 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 配置 VLAN 200 的接口 IP 地址为 128.200.1.180/24。

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 128.200.1.180 24
[AC-Vlan-interface200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan200] quit
```

# 配置 VLAN 300 的接口 IP 地址为 128.130.1.180/24。

```
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 128.130.1.180 24
[AC-Vlan-interface300] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，禁止 VLAN1 通过，配置 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置 DHCP

# 在 AC 上开启 DHCP 服务。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 vlan100 为 AP 动态分配的网段为 128.100.1.0/24，网关地址为 128.100.1.180。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 128.100.1.0 24
[AC-dhcp-pool-vlan100] gateway-list 128.100.1.180
[AC-dhcp-pool-vlan100] quit
```

# 配置 DHCP 地址池 vlan300 为 Client 动态分配的网段为 128.130.1.0/24，网关地址为 128.130.1.180。

```
[AC] dhcp server ip-pool vlan300
[AC-dhcp-pool-vlan300] network 128.130.1.0 24
[AC-dhcp-pool-vlan300] gateway-list 128.130.1.180
[AC-dhcp-pool-vlan300] quit
```

## (3) 配置 WLAN-ESS 接口

# 创建 WLAN-ESS1 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200、VLAN 300 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 300 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

#### (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 缺省情况下，使用 open-system 认证方式。

```
[AC-wlan-st-1] authentication-method open-system
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

#### (5) 配置射频接口并绑定服务模板

# 创建 AP 的管理模板，名称为 officeap，型号名称这里选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 officeap 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 300。。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

# 使能 officeap 的 radio 2。

```
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

# 开启 ARP Snooping 功能后可以在 AC 上显示学习到的 Client 的 IP 地址。

```
[AC] arp-snooping enable
```

### 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

```
[Switch] vlan 300
[Switch-vlan300] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止
VLAN 1 通过，并允许 VLAN 100 和 VLAN 300 通过。
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

### 3.4 验证配置

# 通过命令 **display wlan client** 可以看到 Client 已经接入无线服务 service。

```
[AC] display wlan client
Total Number of Clients          : 1
                                Client Information
SSID: service
-----
MAC Address      User Name      APID/RID IP Address      VLAN
-----
0024-d774-6edc -NA-          1 / 2    128.130.1.3      300
-----
```

#通过命令 **display wlan client verbose** 可以看到 Client 上线的详细信息。

```
[AC] display wlan client verbose
Total Number of Clients          : 1
                                Client Information
-----
MAC Address          : 0024-d774-6edc
User Name            : -NA-
IP Address            : 128.130.1.3
AID                   : 1
AP Name               : officeap
Radio Id              : 2
Antenna Id            : 0
Service Template Number : 1
SSID                  : service
BSSID                 : 80f6-2ee1-44b0
Port                  : WLAN-DBSS1:0
VLAN                  : 300
```

```

State : Running
Power Save Mode : Active
Wireless Mode : 11gn
Channel Band-width : 20MHz
SM Power Save Enable : Disabled
Short GI for 20MHz : Supported
Short GI for 40MHz : Not Supported
STBC TX capability : Not Supported
STBC RX capability : Supported
Support MCS Set : 0,1,2,3,4,5,6,7,8,9,
                  10,11,12,13,14,15

QoS Mode : WMM
Listen Interval (Beacon Interval) : 10
RSSI : 48
Rx/Tx Rate : 6/117
Client Type : PRE-RSNA
Authentication Method : Open System
Authentication Mode : Central
AKM Method : None
4-Way Handshake State : -NA-
Group Key State : -NA-
Encryption Cipher : Clear
Roam Status : Normal
Roam Count : 0
Up Time (hh:mm:ss) : 00:02:02

```

---

### 3.5 配置文件

- AC

```

#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
network 128.100.1.0 mask 255.255.255.0
gateway-list 128.100.1.180
#
dhcp server ip-pool vlan300
network 128.130.1.0 mask 255.255.255.0
gateway-list 128.130.1.180
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1

```

```

service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk pvid vlan 100
port trunk permit vlan 100 300
#
interface Vlan-interface100
ip address 128.100.1.180 255.255.255.0
#
interface Vlan-interface200
ip address 128.200.1.180 255.255.255.0
#
interface Vlan-interface300
ip address 128.130.1.180 255.255.255.0
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 300 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1 vlan-id 300
radio enable
#
dhcp enable
#
arp-snooping enable
#
• Switch:
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2

```

```
port link-mode bridge
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 频谱导航典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤 .....         | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 3 |
| 3.4 验证配置 .....         | 4 |
| 3.5 配置文件 .....         | 4 |
| 4 相关资料 .....           | 6 |



# 1 简介

本文档介绍频谱导航典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

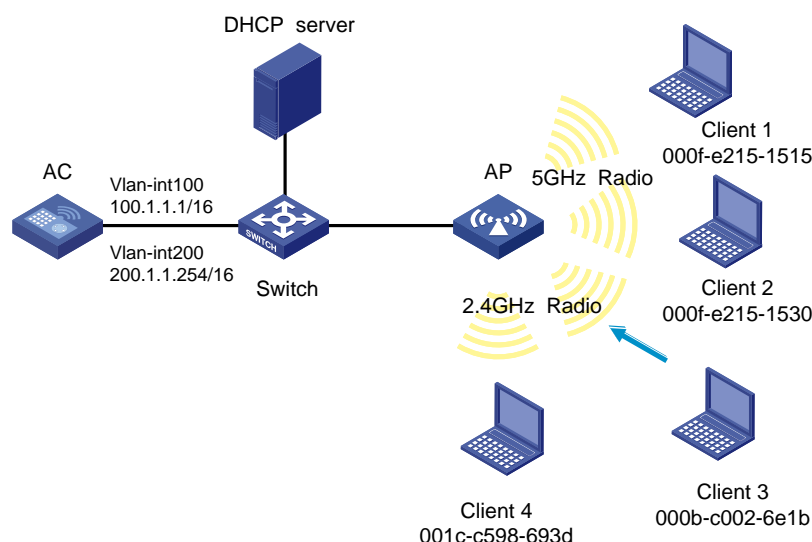
本文档假设您已了解 WLAN RRM 特性。

## 3 配置举例

### 3.1 组网需求

如图1所示，Client 1~Client 4 需要接入 AP，其中 AP 的两个射频模式分别为 5GHz 和 2.4GHz，Client 1、Client 2 与 Client 3 为双频客户端，Client 4 为单频 2.4GHz 客户端。要求：开启频谱导航功能，并配置频谱导航参数，使两个频段上接入的客户端数量相对均衡。

图1 频谱导航配置组网图



### 3.2 配置注意事项

- 由于射频信号在 5GHz 衰减比较大，覆盖范围比 2.4GHz 小，在部署网络时需要注意 5GHz 的覆盖效果。
- 只有同时开启全局和 AP 频谱导航功能，频谱导航功能才能在指定 AP 上生效。

- AP 的频谱导航功能默认处于开启状态。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应,AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 100.1.1.1 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 进入 Vlan-interface200 的接口视图，配置 IP 地址为 200.1.1.1/16。

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 200.1.1.254 255.255.0.0
[AC-Vlan-interface200] quit
```

# 配置 AC 与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型为 Trunk 类型，当前 Trunk 口的 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 和 Client 使用的 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置频谱导航

# 开启全局频谱导航功能。

```
[AC] wlan rrm
[AC-wlan-rrm] band-navigation enable
```

# 配置客户端连接数门限为 2，差值门限为 1。

```
[AC-wlan-rrm] band-navigation balance session 2 gap 1
[AC-wlan-rrm] quit
```

#### (3) 配置无线接入服务

# 创建编号为 1 的 WLAN-ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置端口 WLAN-ESS1 的缺省 VLAN 为 VLAN 200，禁止 VLAN 1 的报文通过并允许 VLAN 200 报文不带 tag 通过。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能端口 WLAN-ESS1 的 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

# 创建一个新的服务模板（明文模板）1，设置服务模板 1 的 SSID 为 service。

```
[AC] wlan service-template 1 clear
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS 接口与该服务模板绑定。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 开启服务模板 1。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

#### (4) 配置接入点信息

# 创建一个 AP 模板，其名称为 officeap，型号名称为 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 将服务模板 1 绑定到 officeap 的 Radio 1，并开启 Radio 1。

```
[AC-wlan-ap-officeap] radio 1
[AC-wlan-ap-officeap-radio-1] service-template 1
[AC-wlan-ap-officeap-radio-1] radio enable
[AC-wlan-ap-officeap-radio-1] quit
```

# 将服务模板 1 绑定到 officeap 的 Radio 2，并开启 Radio 2。

```
[AC-wlan-ap-officeap] radio 2
[AC-wlan-ap-officeap-radio-2] service-template 1
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] return
```

### 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 200，禁止 VLAN 1 通过，允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 200
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/3 接口属性为 Trunk，禁止 VLAN 1 通过，
并允许 VLAN100、VLAN200 通过。
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type trunk
[Switch-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/3] quit
```

### 3.4 验证配置

# Client 1、Client 2 优先接入到 AP 的 5GHz 射频上，Client 4 只能接入到 AP 的 2.4GHz 射频上。此时由于 5GHz 射频上已连接的客户端数量达到门限 2，且 5GHz 射频与 2.4GHz 射频上连接的客户端差值达到门限 1，所以当 Client 3 想接入 AP 时，通过命令 **display wlan client ap officeap radio 2** 发现 Client 3 关联至 AP 的 2.4GHz 射频上。

```
[AC] display wlan client ap officeap radio 2
```

```
Total Number of Clients : 2
```

```
Client Information
```

```
-----
MAC Address User Name APID/RID IP Address VLAN
-----
```

```
000b-c002-6e1b -NA- 1 /2 200.1.1.3 200
001c-c598-693d -NA- 1 /2 200.1.1.4 200
```

### 3.5 配置文件

```
• AC
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan rrm
dot11a mandatory-rate 6 12 24
dot11a supported-rate 9 18 36 48 54
dot11b mandatory-rate 1 2
dot11b supported-rate 5.5 11
```

```

dot11g mandatory-rate 1 2 5.5 11
dot11g supported-rate 6 9 12 18 24 36 48 54
band-navigation balance session 2 gap 1
band-navigation enable
#
wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable
  mac-vlan enable
#
interface Vlan-interface100
  ip address 100.1.1.1 255.255.0.0
#
interface Vlan-interface200
  ip address 200.1.1.254 255.255.0.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk pvid vlan 100
  port trunk permit vlan 100 200
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
    service-template 1
    radio enable
  radio 2
    service-template 1
    radio enable

```

## - Switch

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200

```

```
port trunk pvid vlan 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 实时频谱防护典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 使用限制 .....           | 1 |
| 4 配置举例 .....           | 1 |
| 4.1 组网需求 .....         | 1 |
| 4.2 配置注意事项.....        | 2 |
| 4.3 配置步骤 .....         | 2 |
| 4.3.1 AC 的配置 .....     | 2 |
| 4.3.2 Switch 的配置 ..... | 3 |
| 4.4 验证配置 .....         | 4 |
| 4.5 配置文件 .....         | 5 |
| 5 相关资料 .....           | 6 |



# 1 简介

本文档介绍无线控制器实时频谱防护配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN IDS、WLAN RRM 和 WLAN 高级功能中的频谱分析的相关功能。

## 3 使用限制

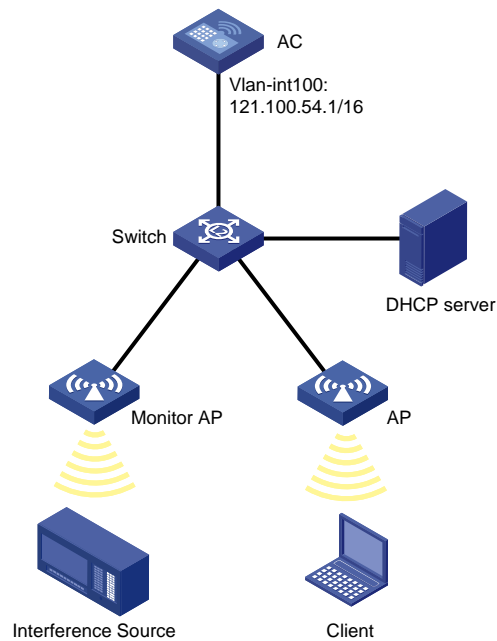
实时频谱防护功能的支持情况与 AP 型号相关，请选择支持该功能的 AP 进行配置，具体的支持情况，请以 AP 设备的实际情况为准。

## 4 配置举例

### 4.1 组网需求

如[图 1](#)所示，现要求通过配置频谱分析功能，Monitor AP 工作在监控模式，实时检测 WLAN 网络中的干扰设备。

图1 频谱分析组网图



## 4.2 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 在监控模式下，AP 不提供接入服务，射频接口会在 800ms 内按照一定顺序进行信道切换，进行一次完整扫描需要 12s。

## 4.3 配置步骤

### 4.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 121.100.54.1 16
[AC-Vlan-interface100] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，PVID 为 100，允许 VLAN 100 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100
```

```
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

## (2) 全局开启频谱分析

# 在 AC 的 RRM 视图下，全局开启频谱分析功能。

```
[AC] wlan rrm
[AC-wlan-rrm] dot11bg spectrum-analysis enable
[AC-wlan-rrm] quit
```

## (3) 配置 Monitor AP

# 创建 Monitor AP 的管理模板，名称为 monitorap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap monitorap model WA2620E-AGN
```

# 设置 Monitor AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-monitorap] serial-id 21023529G007C000020
```

# 配置 Monitor AP 的工作模式为 Monitor。

```
[AC-wlan-ap-monitorap] work-mode monitor
```

## (4) 开启频谱分析功能

# 开启 radio1 上的频谱分析功能，并开启 Monitor AP 的 radio1。

```
[AC-wlan-ap-monitorap] radio 1
[AC-wlan-ap-monitorap-radio-1] spectrum-analysis enable
[AC-wlan-ap-monitorap-radio-1] radio enable
[AC-wlan-ap-monitorap-radio-1] quit
```

# 开启 radio2 上的频谱分析功能，并开启 Monitor AP 的 radio2。

```
[AC-wlan-ap-monitorap] radio 2
[AC-wlan-ap-monitorap-radio-2] spectrum-analysis enable
[AC-wlan-ap-monitorap-radio-2] radio enable
[AC-wlan-ap-monitorap-radio-2] return
```

## 4.3.2 Switch 的配置

# 创建 VLAN 100，其中 VLAN 100 用于转发 AC 和 Monitor AP 间 LWAPP 隧道内的流量。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 Monitor AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过，并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

## 4.4 验证配置

- (1) 配置完成后, 开启干扰设备, 如果干扰设备是微波炉, 十几秒之后, 在 AC 上通过命令行 **display wlan spectrum-analysis device** 可以看到 AP 检测到的微波炉 (Microwave oven) 的信息。

```
<AC> display wlan spectrum-analysis device
SI      : Interference Severity Index
          1-Low Interference, 100-High Interference
```

Interference detected by monitorap Radio2

```
-----
Device ID      : 0x0001
Type           : Microwave oven
SI             : 34
RSSI           : -45
Duty Cycle (%) : 35
Affected Channels : 9,10,11
```

- (2) 如果干扰设备是蓝牙, 检测记录如下:



说明

可以检测为蓝牙的情况为: 1、蓝牙手机之间传输文件; 2、蓝牙耳机拨打电话; 3、蓝牙播放器播放音乐。

```
<AC> display wlan spectrum-analysis device
SI      : Interference Severity Index
          1-Low Interference, 100-High Interference
```

Interference detected by monitorap Radio2

```
-----
Device ID      : 0x0201
Type           : Bluetooth
SI             : 9
RSSI           : -60
Duty Cycle (%) : 7
Affected Channels : 2,10,11
```

- (3) 如果干扰设备是无线摄像头, 检测记录如下:

```
<AC> display wlan spectrum-analysis device
SI      : Interference Severity Index
          1-Low Interference, 100-High Interference
```

Interference detected by monitorap Radio2

```
-----  
Device ID       : 0x0501  
Type           : Video device using fixed frequency  
SI             : 97  
RSSI           : -42  
Duty Cycle (%)  : 94  
Affected Channels : 2,3,4
```

- (4) 通过 **display wlan spectrum-analysis channel-quality** 命令可以查看到当前的信道质量，在 **Interferers** 字段下可以看到各个信道上的干扰设备数量。

```
<AC> display wlan spectrum-analysis channel-quality
```

| Channel Quality |     |         |        |        |             |
|-----------------|-----|---------|--------|--------|-------------|
| AP Name         | RID | Channel | Avg-AQ | Min-AQ | Interferers |
| monitorap       | 2   | 1       | 90     | 90     | 0           |
| monitorap       | 2   | 2       | 92     | 90     | 1           |
| monitorap       | 2   | 3       | 90     | 83     | 1           |
| monitorap       | 2   | 4       | 86     | 79     | 1           |
| monitorap       | 2   | 5       | 77     | 77     | 0           |
| monitorap       | 2   | 6       | 85     | 80     | 0           |
| monitorap       | 2   | 7       | 83     | 83     | 0           |
| monitorap       | 2   | 8       | 84     | 84     | 0           |
| monitorap       | 2   | 9       | 85     | 78     | 0           |
| monitorap       | 2   | 10      | 89     | 88     | 1           |
| monitorap       | 2   | 11      | 91     | 88     | 1           |
| monitorap       | 2   | 12      | 87     | 76     | 1           |
| monitorap       | 2   | 13      | 87     | 67     | 0           |

## 4.5 配置文件

- AC:

```
#  
vlan 100  
#  
wlan rrm  
dot11bg spectrum-analysis enable  
#  
wlan ap-group default_group  
ap monitorap  
#  
interface Vlan-interface100  
ip address 121.100.54.1 255.255.0.0  
#  
interface GigabitEthernet1/0/1  
port link-type trunk  
port trunk permit vlan 100
```

```
port trunk pvid vlan 100
#
wlan ap monitorap model WA2620E-AGN id 1
serial-id 21023529G007C000020
work-mode monitor
radio 1
    spectrum-analysis enable
    radio enable
radio 2
    spectrum-analysis enable
    radio enable
#
```

- **Switch:**

```
#
vlan 100
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 100
    poe enable
#
interface GigabitEthernet1/0/3
    port link-type access
    port access vlan 100
#
```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 授权 ARP 防止终端非法地址接入典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                                   |    |
|-----------------------------------|----|
| 1 简介.....                         | 1  |
| 2 配置前提 .....                      | 1  |
| 3 授权 ARP 功能在 DHCP 服务器上的配置举例 ..... | 1  |
| 3.1 组网需求 .....                    | 1  |
| 3.2 配置步骤 .....                    | 1  |
| 3.2.1 AC 的配置 .....                | 1  |
| 3.2.2 Switch 的配置 .....            | 3  |
| 3.3 验证配置 .....                    | 4  |
| 3.4 配置文件 .....                    | 4  |
| 4 授权 ARP 功能在 DHCP 中继上的配置举例 .....  | 5  |
| 4.1 组网需求 .....                    | 5  |
| 4.2 配置步骤 .....                    | 6  |
| 4.2.1 AC 的配置 .....                | 6  |
| 4.2.2 Switch A 的配置 .....          | 8  |
| 4.2.3 Switch B 的配置 .....          | 8  |
| 4.3 验证配置 .....                    | 9  |
| 4.4 配置文件 .....                    | 9  |
| 5 相关资料 .....                      | 11 |



# 1 简介

本文档介绍授权 ARP 防止终端非法地址接入典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

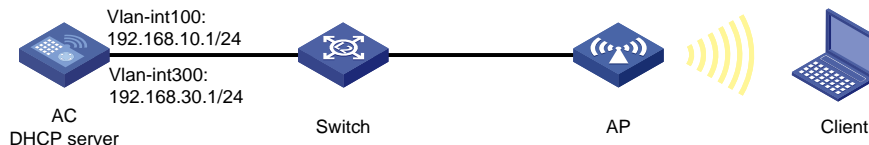
本文档假设您已了解 WLAN、ARP 和 DHCP 特性。

## 3 授权 ARP 功能在 DHCP 服务器上的配置举例

### 3.1 组网需求

如图 1 所示，AC 作为 DHCP 服务器，为 AP 和 Client 分配 IP 地址，现要求配置授权 ARP 功能，实现只有通过 DHCP 服务器获取 IP 地址的用户才能访问网络资源，增加网络安全性。

图1 授权 ARP 功能在 DHCP 服务器上的配置组网图



### 3.2 配置步骤

#### 3.2.1 AC 的配置

##### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.10.1 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 192.168.30.1 24
[AC-Vlan-interface300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 300 的报文通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS 1 接口，并设置端口的链路类型为 Hybrid。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

## (2) 配置 DHCP 服务器

# 创建名为 300 的 DHCP 地址池，并进入其视图。

```
[AC] dhcp server ip-pool 300
```

# 配置 DHCP 地址池 300 为 Client 动态分配的网段为 192.168.30.0/24，网关地址为 192.168.30.1。

```
[AC-dhcp-pool-300] network 192.168.30.0 24
[AC-dhcp-pool-300] gateway-list 192.168.30.1
[AC-dhcp-pool-300] quit
```

# 使能 DHCP 功能。

```
[AC] dhcp enable
```

## (3) 配置授权 ARP 功能

# 进入 VLAN 300 接口视图

```
[AC] interface vlan-interface 300
```

# 配置 DHCP 服务器支持授权 ARP 功能。

```
[AC-Vlan-interface300] dhcp update arp
```

# 使能授权 ARP 功能。

```
[AC-Vlan-interface300] arp authorized enable
[AC-Vlan-interface300] quit
```

## (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC1] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```

[AC1-wlan-st-1] ssid service
# 将 WLAN-ESS 1 接口绑定到服务模板 1。
[AC1-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
(5) 配置 AP
# 创建 AP 的管理模板, 名称为 testap, 型号名称选择 WA2620E-AGN。
[AC1] wlan ap testap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC1-wlan-ap-testap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC1-wlan-ap-testap] radio 2
# 将在 AC 上配置 clear 类型的服务模板 1 与射频 2 进行关联, 同时设置绑定到该射频的 VLAN 为 VLAN 300。
[AC1-wlan-ap-testap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC1-wlan-ap-testap-radio-2] radio enable
[AC1-wlan-ap-testap-radio-2] return

```

### 3.2.2 Switch 的配置

```

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk, PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口链路类型为 Access, 并允许 VLAN 100 通过, 并使能 PoE 功能。
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit

```

### 3.3 验证配置

# 在 Client 成功上线后，在 AC 上通过 **display dhcp server ip-in-use all** 命令查看 DHCP 地址池的地址绑定信息，可以看到 AC 为 Client 动态分配的 IP 地址为 192.168.30.2，绑定 Client 的 MAC 地址为 001e-583f-0895。

```
[AC] display dhcp server ip-in-use all
```

Pool utilization: 0.00%

| IP address   | Client-identifier/<br>Hardware address | Lease expiration     | Type           |
|--------------|----------------------------------------|----------------------|----------------|
| 192.168.30.2 | 001e-583f-0895                         | Mar 29 2013 17:18:50 | Auto:COMMITTED |

# 通过 **display arp all** 命令查看 AC 上的 ARP 表项，授权 ARP 根据 AC 为 Client 动态分配的 IP 地址生成 ARP 表项。

```
[AC] display arp all
```

|              | Type: S-Static | D-Dynamic | A-Authorized |            |
|--------------|----------------|-----------|--------------|------------|
| IP Address   | MAC Address    | VLAN ID   | Interface    | Aging Type |
| 192.168.30.2 | 001e-583f-0895 | 300       | WLAN-DBSS1:0 | N/A A      |

### 3.4 配置文件

- AC:

```
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool 300
    network 192.168.30.0 255.255.255.0
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
interface Vlan-interface100
    ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface300
    ip address 192.168.30.1 255.255.255.0
    arp authorized enable
    dhcp update arp
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 300
    port trunk pvid vlan 100
```

```

#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
 serial-id 21023529G007C000020
 radio 1
 radio 2
 service-template 1 vlan-id 300
 radio enable
#
dhcp enable
#
• Switch:
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 300
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
#

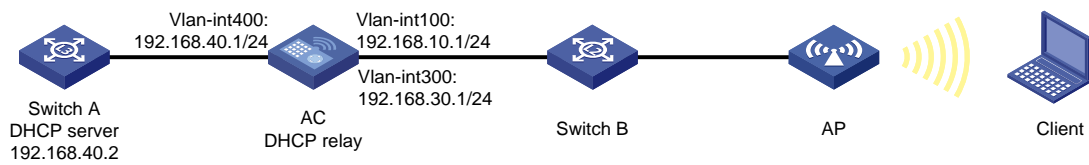
```

## 4 授权 ARP 功能在 DHCP 中继上的配置举例

### 4.1 组网需求

如 [3.1 图 1](#) 所示, Switch A 作为 DHCP 服务器, AC 作为 DHCP 中继, AP 和 Client 通过 AC 从 Switch A 获取 IP 地址, 现要求配置授权 ARP 功能, 实现只有通过 DHCP 服务器获取 IP 地址的用户才能访问网络资源, 增加网络安全性。

图2 授权 ARP 功能在 DHCP 中继上的配置组网图



## 4.2 配置步骤

### 4.2.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```

<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.10.1 24
[AC-Vlan-interface100] quit
  
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```

[AC] vlan 200
[AC-vlan200] quit
  
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```

[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 192.168.30.1 24
[AC-Vlan-interface300] quit
  
```

# 创建 VLAN 400 作为 AC 上行链路的出口 VLAN，并为该接口配置 IP 地址。

```

[AC] vlan 400
[AC-vlan400] quit
[AC] interface vlan-interface 400
[AC-Vlan-interface400] ip address 192.168.40.1 24
[AC-Vlan-interface400] quit
  
```

# 配置 AC 的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 300 的报文通过。

```

[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
  
```

# 创建 WLAN-ESS 1 接口，并设置端口的链路类型为 Hybrid。

```

[AC] interface wlan-ess 1
  
```

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

## (2) 配置 DHCP 中继

# 使能 DHCP 功能。

```
[AC] dhcp enable
```

# 配置 DHCP 服务器组 1 中的服务器的 IP 地址。

```
[AC] dhcp relay server-group 1 ip 192.168.40.2
```

# 配置 VLAN 接口 300 工作在 DHCP 中继模式。

```
[AC] interface vlan-interface 300
```

```
[AC-Vlan-interface300] dhcp select relay
```

# 配置 VLAN 接口 300 与 DHCP 服务器组 1 的归属关系。

```
[AC-Vlan-interface300] dhcp relay server-select 1
```

## (3) 配置授权 ARP 功能

# 配置 DHCP 服务器支持授权 ARP 功能。

```
[AC-Vlan-interface300] dhcp update arp
```

# 使能授权 ARP 功能。

```
[AC-Vlan-interface300] arp authorized enable
```

```
[AC-Vlan-interface300] quit
```

## (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC1] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC1-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC1-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC1-wlan-st-1] service-template enable
```

```
[AC1-wlan-st-1] quit
```

## (5) 配置 AP

# 创建 AP 的管理模板，名称为 testap，型号名称选择 WA2620E-AGN。

```
[AC1] wlan ap testap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC1-wlan-ap-testap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC1-wlan-ap-testap] radio 2
```

# 将在 AC 上配置 clear 类型的服务模板 1 与射频 2 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 300。

```
[AC1-wlan-ap-testap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2。
[AC1-wlan-ap-testap-radio-2] radio enable
[AC1-wlan-ap-testap-radio-2] return
```

#### 4.2.2 Switch A 的配置

# 创建 VLAN 400 作为与 AC 通信的 VLAN，并为该接口配置 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 400
[SwitchA-vlan400] quit
[SwitchA] interface vlan-interface 400
[SwitchA-Vlan-interface400] ip address 192.168.40.2 24
[SwitchA-Vlan-interface400] quit
```

# 配置 Switch 使能 DHCP 服务。

```
[SwitchA] dhcp enable
```

# 创建名为 300 的 DHCP 地址池，配置动态分配的网段为 192.168.30.0/24，网关地址为 192.168.30.1，为 Client 分配 IP 地址。

```
[SwitchA] dhcp server ip-pool 300
[SwitchA-dhcp-pool-300] network 192.168.30.0 24
[SwitchA-dhcp-pool-300] gateway-list 192.168.30.1
[SwitchA-dhcp-pool-300] quit
```

# 配置 Switch A 到 AP 和 Client 所在网段的静态路由。

```
[SwitchA] ip route-static 192.168.30.0 24 192.168.40.1
```

#### 4.2.3 Switch B 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线客户端接入的 VLAN。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] quit
[SwitchB] vlan 300
[SwitchB-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[SwitchB-GigabitEthernet1/0/1] port trunk pvid vlan 100
[SwitchB-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口链路类型为 Access，并允许 VLAN 100 通过，并使能 PoE 功能。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type access
[SwitchB-GigabitEthernet1/0/2] port access vlan 100
[SwitchB-GigabitEthernet1/0/2] poe enable
```



```
[SwitchB-GigabitEthernet1/0/2] quit
```

## 4.3 验证配置

# 在 Client 成功上线后, 通过 **display dhcp relay security** 命令查看 AC 作为 DHCP 中继记录的用户地址表项信息。

```
<AC> display dhcp relay security
IP Address      MAC Address      Type      Interface
192.168.30.2    001e-583f-0895   Dynamic   WLAN-DBSS1:0
--- 1 dhcp-security item(s) found ---
```

# 通过 **display arp all** 命令查看 AC 上的 ARP 表项, 授权 ARP 根据 Switch A 为 Client 动态分配的 IP 地址生成 ARP 表项。

```
[AC] display arp all
Type: S-Static   D-Dynamic   A-Authorized
IP Address      MAC Address      VLAN ID      Interface      Aging Type
192.168.30.2    001e-583f-0895   300          WLAN-DBSS1:0   N/A    A
```

## 4.4 配置文件

- AC:

```
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool 300
network 192.168.30.0 255.255.255.0
gateway-list 192.168.30.1
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface300
ip address 192.168.30.1 255.255.255.0
arp authorized enable
dhcp update arp
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
```

```

port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1 vlan-id 300
radio enable
#
dhcp enable
#

```

- **Switch A:**

```

#
vlan 400
#
dhcp server ip-pool 300
network 192.168.30.0 255.255.255.0
gateway-list 192.168.30.1
#
interface Vlan-interface400
ip address 192.168.40.2 255.255.255.0
#
dhcp enable
#
ip route-static 192.168.30.0 24 192.168.40.1
#

```

- **Switch B:**

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable

```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“三层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“三层技术命令参考”。

# 网站地址过滤典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤.....          | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 4 |
| 3.4 验证配置 .....         | 4 |
| 3.5 配置文件 .....         | 5 |
| 4 相关资料 .....           | 6 |

# 1 简介

本文档介绍无线控制器网站地址过滤的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解网站地址过滤功能。

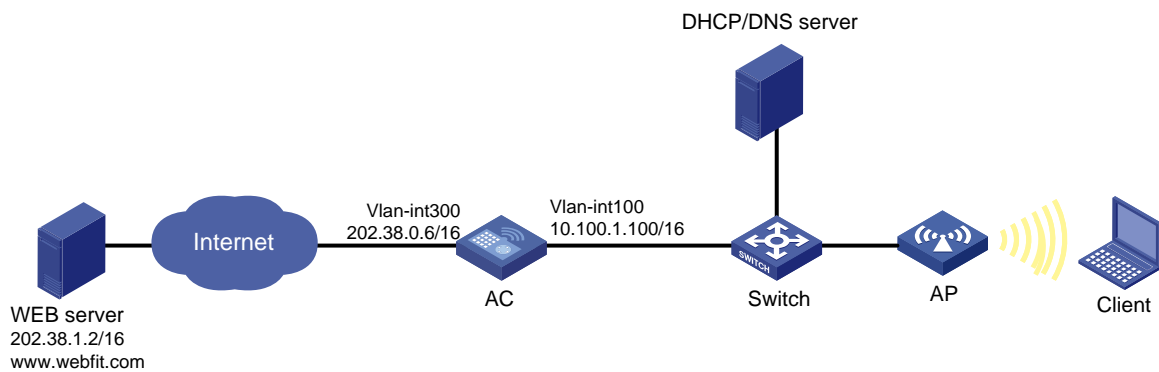
## 3 配置举例

### 3.1 组网需求

如图 1 所示，Client 位于内网，WEB 服务器位于公网，Client 访问 WEB server 的请求数据在 AC 出口上进行地址转换，公网地址范围为 202.38.0.1~202.38.0.5 五个地址，DHCP 和 DNS 部署在同一台服务器上，为 AP 和 Client 分配 IP 地址并提供地址解析服务，具体的应用需求如下：

- Client 可以访问 WEB server，并在 AC 的出接口上做 NAT 地址转换。
- 启用网站地址过滤功能，只允许 Client 访问地址为 www.webfit.com 的网站，同时允许 Client 可以使用 IP 地址的方式访问该网站。

图1 网站地址过滤配置组网图



### 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.100.1.100 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，并配置其 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 202.38.0.6 255.255.0.0
[AC-Vlan-interface300] quit
```

# 配置连接内网接口 GigabitEthernet1/0/1 的链路类型为 Trunk 类型，并配置允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

# 配置连接公网接口 GigabitEthernet1/0/2 的链路类型为 Trunk 类型，并配置仅允许 VLAN 300 通过。

```
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] port link-type trunk
[AC-GigabitEthernet1/0/2] port trunk permit vlan 300
[AC-GigabitEthernet1/0/2] quit
```

#### (2) 配置无线接口

# 创建 WLAN-ESS1 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC-VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

### (3) 配置无线服务

# 创建 **clear** 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 **SSID** 为 **service**。

```
[AC-wlan-st-1] ssid service
```

# 将 **WLAN-ESS1** 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

### (4) 配置射频接口并绑定服务模板

# 创建 **AP** 的管理模板，名称为 **officeap**，型号名称选择 **WA2620E-AGN**，并配置其序列号。

```
[AC] wlan ap officeap model WA2620E-AGN
```

```
[AC-wlan-ap-testap] serial-id 21023529G007C000020
```

# 进入 **radio 2** 射频视图。

```
[AC-wlan-ap-testap] radio 2
```

# 将在 **AC** 上配置的服务模板 1 与射频 2 进行关联。

```
[AC-wlan-ap-testap-radio-2] service-template 1
```

# 使能 **AP** 的 **radio 2**。

```
[AC-wlan-ap-testap-radio-2] radio enable
```

```
[AC-wlan-ap-testap-radio-2] quit
```

```
[AC-wlan-ap-testap] quit
```

### (5) 配置 NAT

# 在 **AC** 上配置一个从 **202.38.0.1~202.38.0.5** 的地址池，地址池索引号为 1。

```
[AC] nat address-group 1 202.38.0.1 202.38.0.5
```

# 在 **AC** 上配置 **ACL** 规则 2001，允许源地址为 **10.110.0.0/16** 的报文通过。

```
[AC] acl number 2001
```

```
[AC-acl-basic-2001] rule permit source 10.100.0.0 0.0.255.255
```

```
[AC-acl-basic-2001] quit
```

# 将地址池与 **ACL** 规则绑定到出接口上。

```
[AC] interface vlan-interface 300
```

```
[AC-Vlan-interface300] nat outbound 2001 address-group 1
```

```
[AC-Vlan-interface300] quit
```

### (6) 配置网站地址过滤

# 使能网站地址过滤功能。

```
[AC] firewall http url-filter host enable
```

# 配置仅允许用户访问 **www.webflt.com**，并设置默认过滤行为为禁止。

```
[AC] firewall http url-filter host url-address permit www.webflt.com
```

```
[AC] firewall http url-filter host default deny
```

# 配置网站地址过滤的 **ACL** 规则。

```
[AC] acl number 2002
```

```
[AC-acl-basic-2002] rule 0 permit source 202.38.1.2 0
```

```
[AC-acl-basic-2002] rule 5 deny source any
```



```
[AC-acl-basic-2002] quit
```

# 配置允许用户以 IP 地址的方式访问该网站，不能访问其它网站。

```
[AC] firewall http url-filter host ip-address deny
```

```
[AC] firewall http url-filter host acl 2002
```

### 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface GigabitEthernet1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface GigabitEthernet1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit.
```

## 3.4 验证配置

# Client 打开浏览器，输入网址 <http://www.webflt.com> 或 <http://202.38.1.2>，可以访问该网站，输入其他网址，无法访问对应的网站。

# 通过 **display firewall http url-filter host verbose** 命令查看网站地址过滤的详细信息。

```
[AC] display firewall http url-filter host verbose
```

```
URL-filter host is enabled.
```

```
Default method: deny.
```

```
The support for IP address: deny.
```

```
The configured ACL group is 2002.
```

```
There are 1 packet(s) being filtered.
```

```
There are 64 packet(s) being passed.
```

# 通过 **display firewall http url-filter host all** 命令查看网站地址过滤的所有条目信息。

```
[AC] display firewall http url-filter host all
```

```
SN   Match-Times      Keywords
-----
1    1                  www.webflt.com
```

## 3.5 配置文件

- AC:

```
#
nat address-group 1 202.38.0.1 202.38.0.5 level 1
#
firewall http url-filter host enable
firewall http url-filter host acl 2002
firewall http url-filter host url-address permit www.webfslt.com
#
acl number 2001
rule 0 permit source 10.100.0.0 0.0.255.255
acl number 2002
rule 0 permit source 202.38.1.2 0
rule 5 deny
#
vlan 100
#
vlan 200
#
vlan 300
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 10.100.1.100 255.255.255.0
#
interface Vlan-interface300
ip address 202.38.0.6 255.255.0.0
nat outbound 2001 address-group 1
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 1 300
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
```

```
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
  service-template 1
  radio enable
#
•   Switch:
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 100 300
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
  poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“三层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“三层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“ACL 和 QoS 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“ACL 和 QoS 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 无线报文捕获典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 2 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 5 |
| 3.5 验证配置 .....         | 6 |
| 3.6 配置文件 .....         | 6 |
| 4 相关资料 .....           | 9 |

# 1 简介

本文介绍了配置 AP 作为侦听、捕获和记录无线报文工具的的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

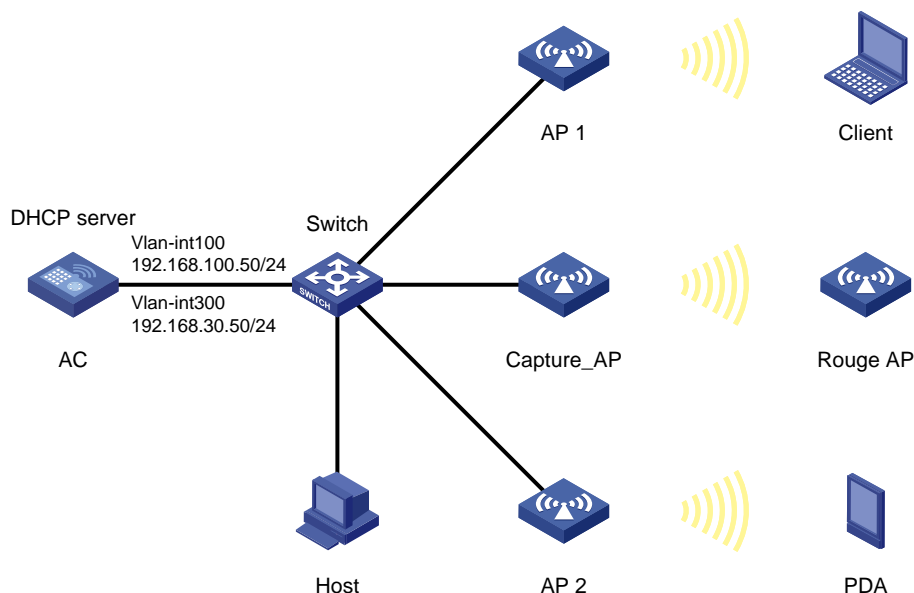
本文档假设您已了解 WLAN 捕获报文的特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，Client 访问无线网络，AC 通过 Switch 和 AP 1、AP 2、Capture\_AP 相连，AC 充当 DHCP 服务器为 AP 和 Client 分配 IP 地址。对于无线环境中有时会出现信号干扰或报文冲突等问题，为了方便管理员对问题进行定位，现要求：在 AC 上指定 Capture\_AP 启动无线捕获功能，侦听网络中的无线报文，并将捕获到的报文生成记录文件保存到 AC 上，并下载到主机 Host。

图1 无线报文捕获组网图



### 3.2 配置思路

为了使 AP 能够捕获无线报文，需要在 AC 上开启 AP 射频的无线捕获功能。

### 3.3 配置注意事项

- 当在 AP 上开启无线捕获功能时，该 AP 正常接入功能无法正常使用。
- 以自动发现方式关联的 AP 不支持无线报文捕获功能。
- 在捕获过程中，系统不允许修改 AP 的工作模式。
- 在捕获过程中，若处于捕获状态的射频被关闭、AP 被删除或者与 AC 连接中断、或者达到报文捕获上限（即：存储捕获报文所需空间超出当前设备存储空间的大小）、或者用户手工停止捕获功能，则捕获操作停止，并在设备的默认存储中将已捕获到的报文保存在指定的记录文件中。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.4 配置步骤

#### 3.4.1 AC 的配置

##### (1) 配置 VLAN 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.100.50 255.255.255.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 192.168.30.50 255.255.255.0
[AC-Vlan-interface300] quit
```

# 配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

##### (2) 配置 DHCP 服务

# 创建名为 **vlan100** 的 DHCP 地址池，动态分配的网段为 **192.168.100.0/24**，网关地址为 **192.168.100.50**。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 192.168.100.0 mask 255.255.255.0
[AC-dhcp-pool-vlan100] gateway-list 192.168.100.50
[AC-dhcp-pool-vlan100] quit
```

# 创建名为 **vlan300** 的 DHCP 地址池，动态分配的网段为 **192.168.30.0/24**，网关地址为 **192.168.30.50**。

```
[AC] dhcp server ip-pool vlan300
[AC-dhcp-pool-vlan300] network 192.168.30.0 mask 255.255.255.0
[AC-dhcp-pool-vlan300] gateway-list 192.168.30.50
[AC-dhcp-pool-vlan300] quit
```

# 使能 DHCP 服务。

```
[AC] dhcp enable
```

### (3) 配置射频接口并绑定服务模板

# 创建型号为 **WA2620E-AGN** 的 AP 模板 **AP1**，序列 ID 设置为 **21023529G007C000020**。

```
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 21023529G007C000020
```

# 进入 **radio 1** 射频视图。

```
[AC-wlan-ap-ap1] radio 1
```

# 将服务模板 **1** 绑定到 **AP 1** 的 **radio 1** 上，设置绑定到射频接口的 **VLAN** 编号为 **VLAN 300**，并使能 **radio 1**。

```
[AC-wlan-ap-ap1-radio-1] service-template 1 vlan-id 300
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
```

# 进入 **radio 2** 射频视图。

```
[AC-wlan-ap-ap1] radio 2
```

# 将服务模板 **1** 绑定到 **AP 1** 的 **radio 2** 上，设置绑定到射频接口的 **VLAN** 编号为 **VLAN 300**，并使能 **radio 2**。

```
[AC-wlan-ap-ap1-radio-2] service-template 1 vlan-id 300
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
```

# 创建型号为 **WA2620E-AGN** 的 AP 模板 **AP2**，序列 ID 设置为 **21023529G007C000021**。

```
[AC] wlan ap ap2 model WA2620E-AGN
[AC-wlan-ap-ap2] serial-id 21023529G007C000021
```

# 进入 **radio 1** 射频视图。

```
[AC-wlan-ap-ap2] radio 1
```

# 将服务模板 **1** 绑定到 **AP 2** 的 **radio 1** 上，设置绑定到射频接口的 **VLAN** 编号为 **VLAN 300**，并使能 **radio 1**。

```
[AC-wlan-ap-ap2-radio-1] service-template 1 vlan-id 300
[AC-wlan-ap-ap2-radio-1] radio enable
[AC-wlan-ap-ap2-radio-1] quit
```

# 进入 **radio 2** 射频视图。

```
[AC-wlan-ap-ap2] radio 2
```



# 将服务模板 1 绑定到 AP 2 的 radio 2 上, 设置绑定到射频接口的 VLAN 编号为 VLAN 300, 并使能 radio 2。

```
[AC-wlan-ap-ap2-radio-2] service-template 1 vlan-id 300
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
```

# 创建型号为 WA2620E-AGN 的 AP 模板 capture\_ap, 序列 ID 设置为 21023529G007C000022。

```
[AC] wlan ap capture_ap model WA2620E-AGN
[AC-wlan-ap-capture_ap] serial-id 21023529G007C000022
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-capture_ap] radio 1
```

# 将服务模板 1 绑定到 capture\_ap 的 radio 1 上, 设置绑定到射频接口的 VLAN 编号为 VLAN 300, 并使能 radio 1。

```
[AC-wlan-ap-capture_ap-radio-1] service-template 1 vlan-id 300
[AC-wlan-ap-capture_ap-radio-1] radio enable
[AC-wlan-ap-capture_ap-radio-1] quit
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-capture_ap] radio 2
```

# 将服务模板 1 绑定到 capture\_ap 的 radio 2 上, 设置绑定到射频接口的 VLAN 编号为 VLAN 300, 并使能 radio 2。

```
[AC-wlan-ap-capture_ap-radio-2] service-template 1 vlan-id 300
[AC-wlan-ap-capture_ap-radio-2] radio enable
[AC-wlan-ap-capture_ap-radio-2] quit
```

#### (4) 配置 WLAN-ESS 接口

# 创建 WLAN-ESS 1, 配置接口的链路类型为 Hybrid。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置接口的缺省 VLAN 为 VLAN 200, 允许发送 VLAN 200 的报文时不带 VLAN Tag。

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 配置接口禁止 VLAN 1 报文通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

#### (5) 配置无线服务

# 创建 clear 方式的无线服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID (服务模板的标识) 为 service1

```
[AC-wlan-st-1] ssid service1
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1 上, 并开启无线服务。

```
[AC-wlan-st-1] bind wlan-ess 1
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

#### (6) 配置无线捕获报文

```
# 配置无线捕获的文件名称为“test”。
[AC] wlan capture file-name test
# 配置无线捕获的报文数量上限为 5000。
[AC] wlan capture packet-limit 5000
# 开启 AP 名称为“capture_ap”的 AP 的 radio 2 的无线捕获功能。
[AC] wlan capture start ap capture_ap radio 2
# 用户可以随时停止捕获，若在捕获过程中停止捕获，则会提示是否保存捕获文件。
[AC] wlan capture stop
Warning: Save the WLAN capture information to an archive file. Continue? [Y/N] :Y
# 捕获记录保存完成后，在 AC 上将会有个名为 test.dmp 的捕获文件，可以通过 FTP 或 TFTP 方式保存捕获记录到主机 Host 上，然后可以使用 OmniPeek 报文解析软件打开该捕获文件。
```

### 3.4.2 Switch 的配置

```
# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线客户端接入的 VLAN。
```

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

```
# 配置 Switch 和 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk，禁止 VLAN 1 报文通过，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。
```

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

```
# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access，当前 Access 口允许 VLAN 100 通过。
```

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

```
# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
```

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

```
# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Access，当前 Access 口允许 VLAN 100 通过。
```

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

```
# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口使能 PoE 功能。
```

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 capture\_ap 相连的 GigabitEthernet1/0/4 接口属性为 Access，当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
```

# 配置 Switch 与 capture\_ap 相连的 GigabitEthernet1/0/4 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
```

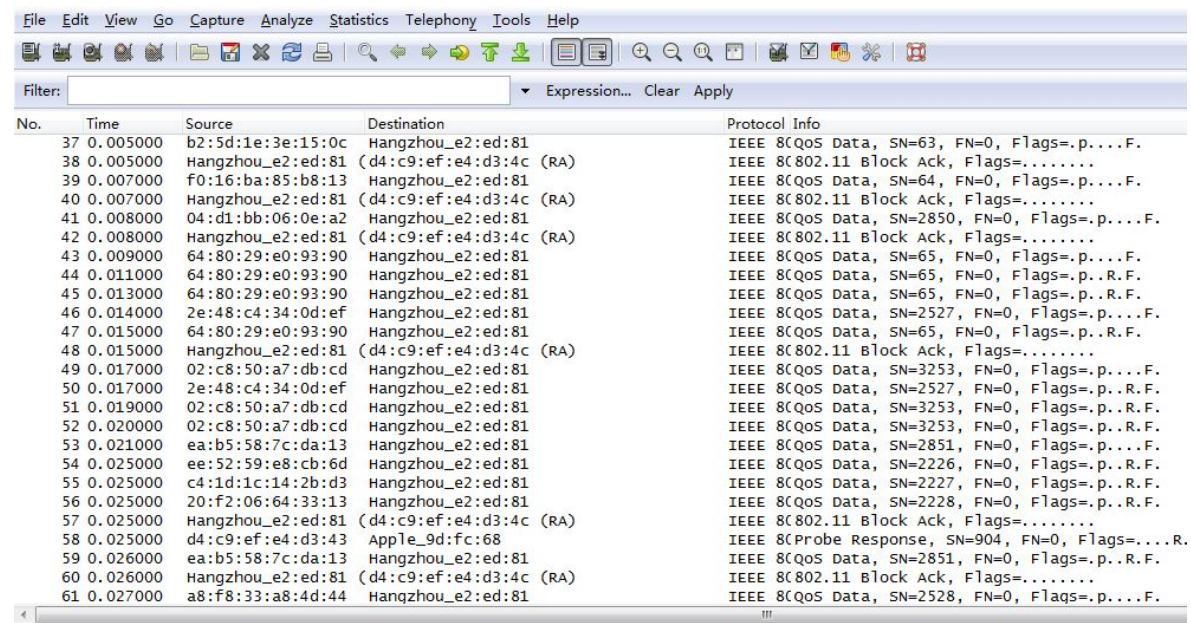
# 配置 Switch 与 Host 相连的 GigabitEthernet1/0/5 接口属性为 Access，当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/5
[Switch-GigabitEthernet1/0/5] port link-type access
[Switch-GigabitEthernet1/0/5] port access vlan 100
[Switch-GigabitEthernet1/0/5] quit
```

## 3.5 验证配置

# 将捕获记录下载到 Host 后，用 OmniPeek 报文解析软件打开该捕获文件，可以看到抓包内容，如图 2 所示。

图2 捕获的无线报文内容



| No. | Time     | Source            | Destination             | Protocol Info                                         |
|-----|----------|-------------------|-------------------------|-------------------------------------------------------|
| 37  | 0.005000 | b2:5d:1e:3e:15:0c | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=63, FN=0, Flags=p...F.           |
| 38  | 0.005000 | Hangzhou_e2:ed:81 | (d4:c9:ef:e4:d3:4c (RA) | IEEE 802.11 Block Ack, Flags=.....                    |
| 39  | 0.007000 | f0:16:ba:85:b8:13 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=64, FN=0, Flags=p...F.           |
| 40  | 0.007000 | Hangzhou_e2:ed:81 | (d4:c9:ef:e4:d3:4c (RA) | IEEE 802.11 Block Ack, Flags=.....                    |
| 41  | 0.008000 | 04:d1:bb:06:0e:a2 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=2850, FN=0, Flags=p...F.         |
| 42  | 0.008000 | Hangzhou_e2:ed:81 | (d4:c9:ef:e4:d3:4c (RA) | IEEE 802.11 Block Ack, Flags=.....                    |
| 43  | 0.009000 | 64:80:29:e0:93:90 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=65, FN=0, Flags=p...F.           |
| 44  | 0.011000 | 64:80:29:e0:93:90 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=65, FN=0, Flags=p...F.           |
| 45  | 0.013000 | 64:80:29:e0:93:90 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=65, FN=0, Flags=p...F.           |
| 46  | 0.014000 | 2e:48:c4:34:0d:ef | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=2527, FN=0, Flags=p...F.         |
| 47  | 0.015000 | 64:80:29:e0:93:90 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=65, FN=0, Flags=p...F.           |
| 48  | 0.015000 | Hangzhou_e2:ed:81 | (d4:c9:ef:e4:d3:4c (RA) | IEEE 802.11 Block Ack, Flags=.....                    |
| 49  | 0.017000 | 02:c8:50:a7:db:cd | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=3253, FN=0, Flags=p...F.         |
| 50  | 0.017000 | 2e:48:c4:34:0d:ef | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=2527, FN=0, Flags=p...F.         |
| 51  | 0.019000 | 02:c8:50:a7:db:cd | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=3253, FN=0, Flags=p...F.         |
| 52  | 0.020000 | 02:c8:50:a7:db:cd | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=3253, FN=0, Flags=p...F.         |
| 53  | 0.021000 | ea:b5:58:7c:da:13 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=2851, FN=0, Flags=p...F.         |
| 54  | 0.025000 | ee:52:59:e8:cb:6d | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=2226, FN=0, Flags=p...F.         |
| 55  | 0.025000 | c4:1d:1c:14:2b:d3 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=2227, FN=0, Flags=p...F.         |
| 56  | 0.025000 | 20:f2:06:64:33:13 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=2228, FN=0, Flags=p...F.         |
| 57  | 0.025000 | Hangzhou_e2:ed:81 | (d4:c9:ef:e4:d3:4c (RA) | IEEE 802.11 Block Ack, Flags=.....                    |
| 58  | 0.025000 | d4:c9:ef:e4:d3:43 | Apple_9d:fc:68          | IEEE 802.11 Probe Response, SN=904, FN=0, Flags=...R. |
| 59  | 0.026000 | ea:b5:58:7c:da:13 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=2851, FN=0, Flags=p...F.         |
| 60  | 0.026000 | Hangzhou_e2:ed:81 | (d4:c9:ef:e4:d3:4c (RA) | IEEE 802.11 Block Ack, Flags=.....                    |
| 61  | 0.027000 | a8:f8:33:a8:4d:44 | Hangzhou_e2:ed:81       | IEEE 802.11 Data, SN=2528, FN=0, Flags=p...F.         |

## 3.6 配置文件

```
• AC:
#
wlan capture packet-limit 5000
wlan capture file-name test
```

```

wlan capture start ap capture_ap radio 2
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
network 192.168.100.0 mask 255.255.255.0
gateway-list 192.168.100.50
#
dhcp server ip-pool vlan300
network 192.168.30.0 mask 255.255.255.0
gateway-list 192.168.30.50
#
wlan service-template 1 clear
ssid servicel
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 192.168.100.50 255.255.255.0
#
interface Vlan-interface300
ip address 192.168.30.50 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
undo port trunk permit vlan 1
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
service-template 1 vlan-id 300
radio enable
radio 2
service-template 1 vlan-id 300
radio enable

```

```
#
wlan ap ap2 model WA2620E-AGN id 2
  serial-id 21023529G007C000021
  radio 1
    service-template 1 vlan-id 300
    radio enable
  radio 2
    service-template 1 vlan-id 300
    radio enable
#
wlan ap capture_ap model WA2620E-AGN id 3
  serial-id 21023529G007C000022
  radio 1
    service-template 1 vlan-id 300
    radio enable
  radio 2
    service-template 1 vlan-id 300
    radio enable
```

```
#
dhcp enable
#
```

- **Switch:**

```
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 300
  undo port trunk permit vlan 1
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/4
  port link-type access
  port access vlan 100
  poe enable
#
```

```
interface GigabitEthernet1/0/5
  port link-type access
  port access vlan 100
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 无线客户端保活和空闲检测典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 1 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 3 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 7 |
| 4 相关资料 .....           | 9 |



# 1 简介

本文介绍了使用无线客户端保活与空闲检测功能的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

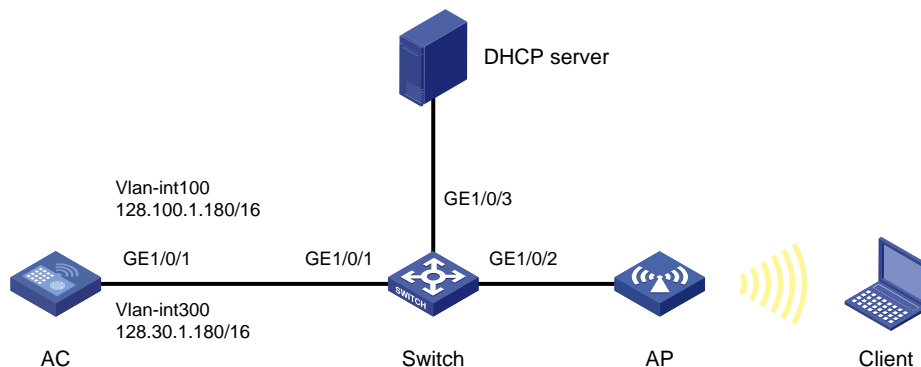
本文档假设您已了解 WLAN 的客户端保活机制和空闲检测机制的特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 通过 Switch 连接 AP 和 DHCP 服务器，DHCP 服务器分别为 Client 和 AP 提供 IP 地址。为了实现及时释放 AC 的客户端列表中失效的客户端信息，现要求：配置 WLAN 的客户端保活机制和空闲检测机制，设置 Client 的保活时间间隔为 3 秒，最大空闲时间为 60 秒。

图1 无线客户端保活与空闲检测功能组网图



### 3.2 配置思路

为实现及时释放 AC 的客户端表项中失效的客户端信息的功能，需要在 AC 的服务模板下配置无线客户端的保活时间间隔和最大空闲时间。

### 3.3 配置注意事项

- 为了能够在 AC 上显示上线 Client 的 IP 地址，需要在 AC 上开启 ARP Snooping 功能。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 128.100.1.180 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan200] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 128.30.1.180 16
[AC-Vlan-interface300] quit
```

# 配置 AC 连接 Switch 的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，设置 PVID 为 VLAN 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS 1 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS 1 接口类型为 Hybrid 类型。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

#### (2) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(3) 配置射频接口并绑定服务模板
# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。
[AC] wlan ap officeap model WA2620E-AGN
# 设置 officeap 的序列号为 210235A29G007C000020。
[AC-wlan-ap-officeap] serial-id 210235A29G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行绑定，设置绑定到射频接口的 VLAN 编号为 VLAN 300。
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 officeap 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
(4) 配置无线客户端的保活机制和空闲检测机制
# 设置无线客户端的保活时间间隔为 3 秒。
[AC-wlan-ap-officeap] client keep-alive 3
# 设置无线客户端最大空闲时间为 60 秒。
[AC-wlan-ap-officeap] client idle-timeout 60
[AC-wlan-ap-officeap] quit
(5) 开启 ARP Snooping 功能
[AC] arp snooping enable
```

### 3.4.2 Switch 的配置

```
# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线客户端接入的 VLAN。
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk，禁止 VLAN 1 报文通过，设置 PVID 为 VLAN 100，允许 VLAN 100 和 VLAN 300 通过。
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

## 3.5 验证配置

# 通过命令 **display wlan ap name officeap verbose** 可以看到无线客户端配置的保活时间间隔为 3 秒，空闲时间为 60 秒。

```
<AC> display wlan ap name officeap verbose
```

```
AP Profile: officeap
```

```
-----
APID                               : 1
Auto AP                            : NO
AP System Name                     : Not Configured
Map Configuration                   : Not Configured
State                              : Run
Up Time(hh:mm:ss)                  : 00:01:54

Model                              : WA2620E-AGN
Serial-ID                          : 210235A29G007C000020
AC IP Address                      : 128.100.1.180
AP IP Address                      : 128.100.0.4

H/W Version                        : Ver.A
S/W Version                        : V100R001B96D037
Boot-Rom Version                   : 2.02
Description                        : Not Configured

Connection Type                    : Master
Peer AC MAC Address                : -NA-
Priority Level                      : 4
Echo Interval(s)                   : 10
Statistics report Interval(s)      : 50

Cir(Kbps)                         : -NA-
Cbs(Bytes)                        : -NA-
```

Jumboframe Threshold : Disable  
  
 Transmitted control packets : 90  
 Received control packets : 90  
 Transmitted data packets : 79999  
 Received data packets : 73  
  
 Echo Average Delay(ms) : 13  
 Echo Request Count : 10  
 Echo Response Loss Count : 0  
  
 Configuration Failure Count : 0  
 Last Failure Reason :  
  
 Last Reboot Reason : Tunnel Initiated  
  
 Latest IP Address : 128.100.0.4  
 Tunnel Down Reason : Response Timer Expire  
 Connection Count : 67  
 AP-Group Name : 1

-----

AP Mode : Split  
 AP operation mode : Normal  
 Portal Service : Disable  
 Device Detection : Disable  
 Maximum Number of Radios : 2  
 Current Number of Radios : 2  
 Client Keep-alive Interval (s): 3  
 Client Idle Interval(s) : 60  
 Broadcast-probe Reply Status : Enable  
 Radio 1:  
     Basic BSSID : 5866-ba94-71e0  
     Current BSS Count : 0  
     Running Clients Count : 0  
     Wireless Mode : 11an  
     Client Dot11n-only : Disabled  
     Channel Band-width : 20/40MHz  
     Secondary Channel Offset : SCN  
     HT Protection Mode : no protection  
     Short GI for 20MHz : Supported  
     Short GI for 40MHz : Supported  
     Mandatory MCS Set :  
     Support MCS Set : 0,1,2,3,4,5,6,7,8,9,  
                             10,11,12,13,14,15,16,17,18,19,  
                             20,21,22,23  
  
 A-MSDU : Enabled  
 A-MPDU : Enabled

```

Green Energy Management      : Disabled
MIMO                         : Default
STBC                         : Enabled
LDPC                         : Disabled
Configured Channel           : auto
Configured Power (dBm)       : 20
Radio Policy                  : default_rp
Mesh Policy                   : default_mp_plcy
ANI Support                   : Enable
Admin State                   : DOWN
Physical State                : UP
Operational Rates (Mbps):
    6                         : mandatory
    9                         : supported
   12                         : mandatory
   18                         : supported
   24                         : mandatory
   36                         : supported
   48                         : supported
   54                         : supported
Radar detected Channels      : None
Antenna Type                  : Internal Antenna
Resource Using Ratio (%)     : 0
Noise Floor (dBm)           : 0
Radio 2:
    Basic BSSID                : 5866-ba94-71f0
    Current BSS Count          : 1
    Running Clients Count      : 1
    Wireless Mode              : 11gn
    Client Dot11n-only         : Disabled
    Channel Band-width         : 20MHz
    Secondary Channel Offset    : SCN
    HT Protection Mode          : no protection
    Short GI for 20MHz          : Supported
    Short GI for 40MHz          : Supported
    Mandatory MCS Set          :
    Support MCS Set            : 0,1,2,3,4,5,6,7,8,9,
                                10,11,12,13,14,15,16,17,18,19,
                                20,21,22,23
    A-MSDU                     : Enabled
    A-MPDU                     : Enabled
    Green Energy Management     : Disabled
    MIMO                       : Default
    STBC                       : Enabled
    LDPC                       : Disabled
    Configured Channel          : auto(11)
    Configured Power (dBm)     : 20
    Interference (%)            : 54

```

```

Channel Load (%)           : 54
Utilization (%)           : 0
Co-channel Neighbor Count  : 3
Channel Health            : Bad
Preamble Type             : short
Radio Policy              : default_rp
Service Template          : 1
SSID                      : service
Port                      : WLAN-DBSS1:2147
Mesh Policy               : default_mp_plcy
ANI Support               : Enable
11g Protection           : Disable
Admin State               : UP
Physical State            : UP
Operational Rates (Mbps):
  1                       : mandatory
  2                       : mandatory
  5.5                     : mandatory
  6                       : supported
  9                       : supported
  11                      : mandatory
  12                      : supported
  18                      : supported
  24                      : supported
  36                      : supported
  48                      : supported
  54                      : supported
Radar detected Channels   : None
Antenna Type              : Internal Antenna
Resource Using Ratio (%)  : 23
Noise Floor (dBm)        : -110

```

-----

# 在 AC 上配置允许日志信息输出到监视终端。

```
<AC> terminal monitor
```

# 将 client 关机或者断电，使得 client 不能对 AC 发送下线通知。

# 如果在保活时间间隔周期 3 秒周期后，AC 未收到 Client 的 Deauth 通知，那么 AC 就会主动删除对应 Client 表项，通过命令行自动打印的信息验证 Client 被 AC 下线。

```
%Nov 28 09:50:54:441 2013 AC WMAC/6/WMAC_CLIENT_GOES_OFFLINE: Client 000f-e212-8410
disconnected from WLAN service. Reason code is 1.
```

# 将 client 重新上线，然后 60 秒之内不发送任何数据。在 60 秒周期内 AC 没有收到 Client 发送的数据报文，AC 就会将 Client 下线，通过命令行自动打印的信息验证 Client 被 AC 下线。

```
%Nov 27 15:42:39:209 2013 AC WMAC/6/WMAC_CLIENT_GOES_OFFLINE: Client 0021-632f-e17d
disconnected from WLAN service. Reason code is 4.
```

## 3.6 配置文件

- AC:

```

#
arp snooping enable
#
vlan 100
#
vlan 200
#
vlan 300
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 300
    undo port trunk permit vlan 1
    port trunk pvid vlan 100
#
interface Vlan-interface100
    ip address 128.100.1.180 255.255.0.0
#
interface Vlan-interface300
    ip address 128.30.1.180 255.255.0.0
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
    serial-id 210235A29G007C000020
    client idle-timeout 60
    client keep-alive 3
    radio 1
    radio 2
        service-template 1 vlan-id 300
    radio enable
#
●    Switch:
#
vlan 100
#
vlan 300
#

```



```
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 300
 undo port trunk permit vlan 1
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
#
interface GigabitEthernet1/0/3
 port link-type access
 port access vlan 100
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 无线控制器 AP 自动注册和认证典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项.....        | 2 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 4 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 5 |
| 4 相关资料 .....           | 7 |

# 1 简介

本文档介绍 AP 自动注册和认证特性典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 接入中的自动 AP 的相关功能。

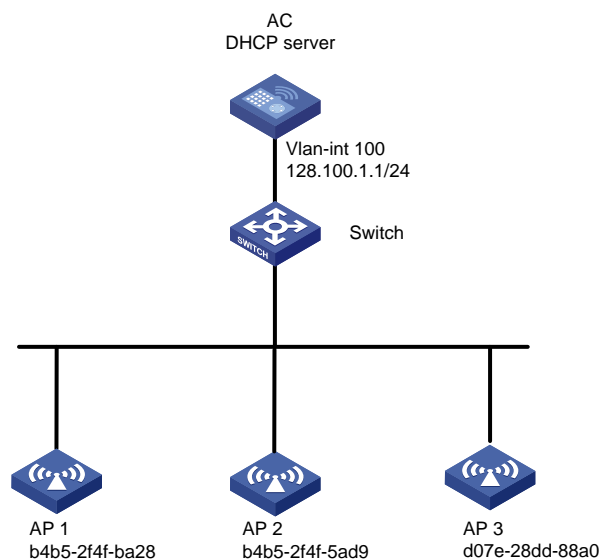
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，AC 和 AP 工作在一个局域网内，AC 作为 DHCP 服务器为 AP 分配 IP 地址，现要求通过配置自动 AP 认证功能，实现如下效果：

- AP3 可以完成自动 AP 认证，AP2 无法完成认证，不能接入网络
- AP1 需要通过手工认证接入无线网络

图1 AP 自动注册和认证特性典型配置组网图



### 3.2 配置思路

- 为了实现自动 AP 认证，需要选择认证方式，本例使用 MAC 地址方式进行认证。

- 为了区分允许自动认证和禁止自动认证的 AP，需要定义 WLAN-AP ACL，分别匹配这些 AP 的 MAC 地址。

### 3.3 配置注意事项

- 配置对未认证的自动 AP 进行手工认证前，需要使用 **wlan ap-authentication acl** 命令使用 ACL 对自动 AP 进行认证。
- AC 会以 AP 的 MAC 地址来命名上线的自动 AP。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.4 配置步骤

#### 3.4.1 AC 的配置

##### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 128.100.1.1 24
[AC-Vlan-interface100] quit
```

# 创建 WLAN-ESS1 接口。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，配置 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100
[AC-GigabitEthernet1/0/1] quit
```

##### (2) 配置 DHCP

# 在 AC 上开启 DHCP 服务。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 vlan100 为 AP 动态分配的网段为 128.100.1.0/24，网关地址为 128.100.1.1。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 128.100.1.0 24
[AC-dhcp-pool-vlan100] gateway-list 128.100.1.1
[AC-dhcp-pool-vlan100] quit
```

##### (3) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

#### (4) 配置 AP 组

```
# 配置 AP 缺省组 default_group。
[AC] wlan ap-group default_group
# 将服务模板 1 映射到 AP 组内成员 AP 的 5GHz 射频。
[AC-ap-group-default_group] dot11a service-template 1
# 将服务模板 1 映射到 AP 组内成员 AP 的 2.4GHz 射频。
[AC-ap-group-default_group] dot11bg service-template 1
# 开启 AP 组名为 default_group 内成员 AP 的 5GHz 射频。
[AC-ap-group-default_group] dot11a radio enable
# 开启 AP 组名为 default_group 内成员 AP 的 2.4GHz 射频。
[AC-ap-group-default_group] dot11bg radio enable
[AC-ap-group-default_group] quit
```

#### (5) 配置自动 AP 并开启自动 AP 认证功能

```
# 配置自动 AP。
[AC] wlan auto-ap enable
# 开启自动 AP 认证功能。
[AC] wlan ap-authentication enable
# 缺省情况下，使用 MAC 地址对自动 AP 进行认证。
[AC] wlan ap-authentication method mac-address
# 创建 ACL 200 作为自动 AP 认证的 WLAN-AP ACL。
[AC] acl number 200
# 制定如下规则：允许 AP 3（MAC 地址为 d07e-28dd-88a0）接入 AC；禁止 AP 2（MAC 地址为 b4b5-2f4f-5ad9）接入 AC。
[AC-acl-ap-200] rule permit mac d07e-28dd-88a0 ffff-ffff-ffff
[AC-acl-ap-200] rule deny mac b4b5-2f4f-5ad9 ffff-ffff-ffff
[AC-acl-ap-200] quit
# 使用 ACL 200 对自动 AP 进行认证。
[AC] wlan ap-authentication acl 200
```

#### (6) 对未认证的自动 AP 进行手工认证

```
# 配置对未认证的自动 AP 进行手工认证。
[AC] wlan ap-authentication accept ap unauthenticated all
# 配置将自动 AP 转化为固定 AP。
[AC] wlan auto-ap persistent all
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量和无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止 VLAN 1 通过，允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 AP 3 相连的 GigabitEthernet1/0/4 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
```

# 配置 Switch 与 AP 3 相连的 GigabitEthernet1/0/4 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
```

## 3.5 验证配置

# 在 AC 上通过命令行 **display wlan ap all** 查看 AP 状态。AP 3（MAC 地址为 d07e-28dd-88a0）匹配 ACL 规则上线，AP 1（b4b5-2f4f-ba28）通过手工认证也关联到 AC 上线，而 AP 2（b4b5-2f4f-5ad9）匹配 ACL 规则不上线。

```
<AC> display wlan ap all
Total Number of APs configured          : 0
Total Number of configured APs connected : 0
Total Number of auto APs connected      : 2
```

```

AP Profiles
State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
        C = Config, R = Run, KU = KeyUpdate, KC = KeyCfm
        M = Master, B = Backup

```

| AP Name        | State | Model       | Serial-ID           |
|----------------|-------|-------------|---------------------|
| b4b5-2f4f-ba28 | R/M   | WA2620E-AGN | 21023529G007C000020 |
| d07e-28dd-88a0 | R/M   | WA2620E-AGN | 21023529G007C000021 |

# 在 AC 上通过命令行 **wlan ap-authentication accept ap unauthenticated all** 对未认证的自动 AP 进行手工认证，使自动 AP 的状态从“未认证”转化为“已认证”，并将自动 AP 的 MAC 地址加入指定的 ACL 编号中，生成对应的 **rule permit** 规则，认证后的自动 AP 可以提供无线服务。在 AC 上通过命令行 **display acl 200** 查看新生成的 ACL 规则。

```

[AC] display acl 200
WLAN-AP ACL 200, 3 rules,
ACL's step is 5
rule 0 permit mac d07e-28dd-88a0 ffff-ffff-ffff(2 times matched)
rule 5 deny mac b4b5-2f4f-5ad9 ffff-ffff-ffff(26 times matched)
rule 10 permit mac b4b5-2f4f-ba28 ffff-ffff-ffff

```

# 使用 **wlan ap** 命令在 AC 上进入 AP 1: b4b5-2f4f-ba28 模板视图，查看是否继承 ap-group 组的配置。

```

[AC-wlan-ap-b4b5-2f4f-ba28] display this
#
wlan ap b4b5-2f4f-ba28 model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
service-template 1
radio enable
radio 2
service-template 1
radio enable
#
return

```

## 3.6 配置文件

```

• AC
#
wlan auto-ap enable
#
password-recovery enable
#
acl number 200
rule 0 permit mac d07e-28dd-88a0 ffff-ffff-ffff
rule 5 deny mac b4b5-2f4f-5ad9 ffff-ffff-ffff
#

```



```

vlan 100
#
dhcp server ip-pool vlan100
network 128.100.1.0 mask 255.255.255.0
gateway-list 128.100.1.1
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
wlan ap-group default_group
ap d07e-28dd-88a0
dot11a service-template 1
dot11bg service-template 1
dot11a radio enable
dot11bg radio enable
#
interface Vlan-interface100
ip address 128.100.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk permit vlan 100
#
interface WLAN-ESS1
#
wlan ap-authentication enable
wlan ap-authentication acl 200
#
dhcp enable
#

```

## - Switch

```

#
vlan 100
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
poe enable

```

```
#
interface GigabitEthernet1/0/3
port link-mode bridge
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/4
port link-mode bridge
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 无线控制器 VRRP 热备管理 AP 典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |    |
|------------------------|----|
| 1 简介.....              | 1  |
| 2 配置前提 .....           | 1  |
| 3 配置举例 .....           | 1  |
| 3.1 组网需求 .....         | 1  |
| 3.2 配置思路 .....         | 2  |
| 3.3 配置注意事项.....        | 2  |
| 3.4 配置步骤 .....         | 2  |
| 3.4.1 AC 1 的配置 .....   | 2  |
| 3.4.2 AC 2 的配置 .....   | 4  |
| 3.4.3 Switch 的配置 ..... | 6  |
| 3.5 验证配置 .....         | 6  |
| 3.6 配置文件 .....         | 8  |
| 4 相关资料 .....           | 10 |

# 1 简介

本文档介绍了无线控制器 VRRP 热备管理 AP 典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 接入、VRRP 热备等特性。

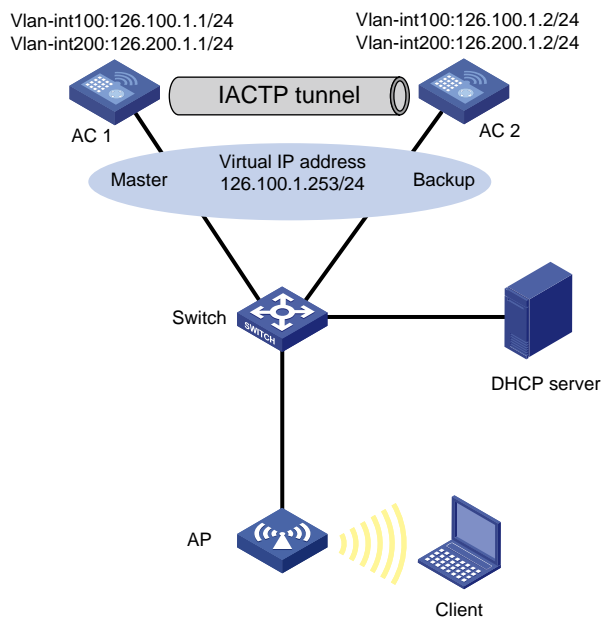
## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，为了提高网络中 AC 的可靠性，现要求使用 VRRP 热备功能，将 AC 1 和 AC 2 组成一台虚拟 AC，为 Client 提供无线接入服务。具体要求如下：

- AC 1 正常工作的情况下，Client 通过 AC 1 访问网络。
- 当 AC 1 发生故障时，Client 切换至 AC 2 上，保证业务流量在切换过程中不会中断。

图1 VRRP 热备管理 AP 典型组网图



## 3.2 配置思路

- 为了让 AC 1 成为 VRRP 备份组中的 Master，需要为 AC 1 配置较高的优先级。
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。
- 当备份组中的角色发生变化时，为了保证网络流量不会中断，需要在 AC 1 和 AC 2 之间建立 IACTP 隧道，并通过 AP 信息备份以及 Client 备份功能，使 AC 之间可以同步备份 AP 和 Client 的信息。

## 3.3 配置注意事项

- 两台 AC 需保证 WLAN 相关的特性配置一致，否则可能出现备份失败等问题。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 需要确保在完成 VRRP 配置、IACTP 隧道、开启客户端信息备份功能后，再开启 AP 信息备份功能。
- 需要在配置 IACTP 隧道的源 IP 地址后才可以开启隧道。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

#### (1) 配置 AC 1 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 1 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道，同时用于与 AC 2 建立 VRRP 备份组和 IACTP 隧道。

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 126.100.1.1 24
[AC1-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 126.200.1.1 24
[AC1-Vlan-interface200] quit
```

# 配置 AC 1 与 Switch 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 200 的报文通过。

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC1-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC1-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS 1 接口

```
[AC1] interface wlan-ess 1
```

# 配置 WLAN-ESS 1 接口链路类型为 Hybrid。

```
[AC1-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，允许 VLAN 200 不带 tag 通过。

```
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC1-WLAN-ESS1] mac-vlan enable
```

```
[AC1-WLAN-ESS1] quit
```

## (2) 配置 VRRP 功能

# 创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IP 地址为 126.100.1.253。

```
[AC1] interface vlan-interface 100
```

```
[AC1-Vlan-interface100] vrrp vrid 1 virtual-ip 126.100.1.253
```

# 设置 AC 1 在备份组 1 中的优先级为 110。

```
[AC1-Vlan-interface100] vrrp vrid 1 priority 110
```

# 设置 AC 1 工作在抢占模式，抢占延迟时间为 6 秒。

```
[AC1-Vlan-interface100] vrrp vrid 1 preempt-mode timer delay 6
```

```
[AC1-Vlan-interface100] quit
```

## (3) 配置 IACTP 隧道

# 创建 IACTP 隧道 1，并进入其视图。

```
[AC1] wlan mobility-group 1
```

# 配置 IACTP 隧道 1 的源 IP 地址为 AC 1 的 IP 地址 126.100.1.1。

```
[AC1-wlan-mg-1] source ip 126.100.1.1
```

# 配置 IACTP 隧道 1 的成员 IP 地址为 AC 2 的 IP 地址 126.100.1.2。

```
[AC1-wlan-mg-1] member ip 126.100.1.2
```

# 开启 IACTP 隧道。

```
[AC1-wlan-mg-1] mobility-group enable
```

```
[AC1-wlan-mg-1] quit
```

# 开启客户端信息备份功能。

```
[AC1] wlan backup-client enable
```

# 开启 AP 信息备份功能。

```
[AC1] wlan backup-ap enable
```

## (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC1] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC1-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC1-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC1-wlan-st-1] service-template enable
```

```
[AC1-wlan-st-1] quit
```

### (5) 配置 AP

# 创建 AP 的管理模板，名称为 **testap**，型号名称选择 **WA2620E-AGN**。

```
[AC1] wlan ap testap model WA2620E-AGN
```

# 设置 AP 的序列号为 **21023529G007C000020**。

```
[AC1-wlan-ap-testap] serial-id 21023529G007C000020
```

# 进入 **radio 2** 射频视图。

```
[AC1-wlan-ap-testap] radio 2
```

# 将在 AC 上配置 **clear** 类型的服务模板 **1** 与射频 **2** 进行关联。

```
[AC1-wlan-ap-testap-radio-2] service-template 1
```

# 使能 AP 的 **radio 2**。

```
[AC1-wlan-ap-testap-radio-2] radio enable
```

```
[AC1-wlan-ap-testap-radio-2] return
```

## 3.4.2 AC 2 的配置

### (1) 配置 AC 2 的接口

# 创建 **VLAN 100** 及其对应的 **VLAN** 接口，并为该接口配置 **IP** 地址。**AC 2** 将使用该接口的 **IP** 地址与 **AP** 建立 **LWAPP** 隧道，同时用于与 **AC 1** 建立 **VRRP** 备份组和 **IACTP** 隧道。

```
<AC2> system-view
```

```
[AC2] vlan 100
```

```
[AC2-vlan100] quit
```

```
[AC2] interface vlan-interface 100
```

```
[AC2-Vlan-interface100] ip address 126.100.1.2 24
```

```
[AC2-Vlan-interface100] quit
```

# 创建 **VLAN 200** 作为 **WLAN-ESS** 接口的缺省 **VLAN**，同时作为 **Client** 接入的业务 **VLAN**，并为该接口配置 **IP** 地址。

```
[AC2] vlan 200
```

```
[AC2-vlan200] quit
```

```
[AC2] interface vlan-interface 200
```

```
[AC2-Vlan-interface200] ip address 126.200.1.2 24
```

```
[AC2-Vlan-interface200] quit
```

# 配置 **AC 2** 与 **Switch** 相连的 **GigabitEthernet1/0/1** 接口链路类型为 **Trunk**，**PVID** 为 **100**，允许 **VLAN 100** 和 **VLAN 200** 的报文通过。

```
[AC2] interface gigabitethernet 1/0/1
```

```
[AC2-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[AC2-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[AC2-GigabitEthernet1/0/1] quit
```

# 创建 **WLAN-ESS 1** 接口

```
[AC2] interface wlan-ess 1
```

# 配置 **WLAN-ESS 1** 接口链路类型为 **Hybrid**。

```
[AC2-WLAN-ESS1] port link-type hybrid
```

# 配置当前 **Hybrid** 端口的 **PVID** 为 **VLAN 200**，允许 **VLAN 200** 不带 **tag** 通过。

```
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
```



# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC2-WLAN-ESS1] mac-vlan enable
```

```
[AC2-WLAN-ESS1] quit
```

## (2) 配置 VRRP

# 创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IP 地址为 126.100.1.253，AC 2 在备份组 1 中的优先级取缺省值 100。

```
[AC2] interface vlan-interface 100
```

```
[AC2-Vlan-interface100] vrrp vrid 1 virtual-ip 126.100.1.253
```

# 设置 AC 2 工作在抢占方式，抢占延迟时间为 6 秒。

```
[AC2-Vlan-interface100] vrrp vrid 1 preempt-mode timer delay 6
```

```
[AC2-Vlan-interface100] quit
```

## (3) 配置 IACTP 隧道

# 创建 IACTP 隧道 1，并进入其视图。

```
[AC2] wlan mobility-group 1
```

# 配置 IACTP 隧道 1 的源 IP 地址为 AC 2 的 IP 地址 126.100.1.2。

```
[AC2-wlan-mg-1] source ip 126.100.1.2
```

# 配置配置 IACTP 隧道 1 的成员 IP 地址为 AC 1 的 IP 地址 126.100.1.1。

```
[AC2-wlan-mg-1] member ip 126.100.1.1
```

# 开启 IACTP 隧道。

```
[AC2-wlan-mg-1] mobility-group enable
```

```
[AC2-wlan-mg-1] quit
```

# 开启客户端信息备份功能。

```
[AC2] wlan backup-client enable
```

# 开启 AP 信息备份功能。

```
[AC2] wlan backup-ap enable
```

## (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC2] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC2-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC2-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC2-wlan-st-1] service-template enable
```

```
[AC2-wlan-st-1] quit
```

## (5) 配置 AP

# 创建 AP 的管理模板，名称为 testap，型号名称选择 WA2620E-AGN。

```
[AC2] wlan ap testap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC2-wlan-ap-testap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC2-wlan-ap-testap] radio 2
```

# 将在 AC 上配置 clear 类型的服务模板 1 与射频 2 进行关联。

```
[AC2-wlan-ap-testap-radio-2] service-template 1
# 使能 AP 的 radio 2。
[AC2-wlan-ap-testap-radio-2] radio enable
[AC2-wlan-ap-testap-radio-2] return
```

### 3.4.3 Switch 的配置

# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 200 为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 1 相连的 GigabitEthernet1/0/1 接口属性 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AC 2 相连的 GigabitEthernet1/0/2 接口属性 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/4 接口属性为 Access，并允许 VLAN 100 通过，并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
```

## 3.5 验证配置

- (1) 当 MAC 地址为 001f-3b03-781f 的 Client 通过 SSID 为 service 的无线服务上线时，在 AC 1 上通过 **display wlan ap all** 命令可以查看 AP 和 Client 的信息。

```

<AC1> display wlan ap all
Total Number of APs configured          : 1
Total Number of configured APs connected : 1
Total Number of auto APs connected      : 0

          AP Profiles
State : I = Idle,  J = Join, JA = JoinAck,  IL = ImageLoad
       C = Config, R = Run,  KU = KeyUpdate, KC = KeyCfm
       M = Master, B = Backup

```

| AP Name | State Model     | Serial-ID           |
|---------|-----------------|---------------------|
| testap  | R/M WA2620E-AGN | 21023529G007C000020 |

```

<AC1> display wlan client
Total Number of Clients          : 1

          Client Information
SSID: service

```

| MAC Address    | User Name | APID/RID | IP Address  | VLAN |
|----------------|-----------|----------|-------------|------|
| 001f-3b03-781f | -NA-      | 1 /2     | 126.200.1.3 | 200  |

(2) 此时在 AC 2 上通过 **display wlan ap all** 命令查看到 AP 和 Client 的信息，可以看见 AP 和 Client 信息已经备份到 AC 2。

```

<AC2> display wlan ap all
Total Number of APs configured          : 1
Total Number of configured APs connected : 1
Total Number of auto APs connected      : 0

          AP Profiles
State : I = Idle,  J = Join, JA = JoinAck,  IL = ImageLoad
       C = Config, R = Run,  KU = KeyUpdate, KC = KeyCfm
       M = Master, B = Backup

```

| AP Name | State Model     | Serial-ID           |
|---------|-----------------|---------------------|
| testap  | R/B WA2620E-AGN | 21023529G007C000020 |

```

<AC2> display wlan client
Total Number of Clients          : 1

          Client Information
SSID: service

```

| MAC Address    | User Name | APID/RID | IP Address  | VLAN |
|----------------|-----------|----------|-------------|------|
| 001f-3b03-781f | -NA-      | 1 /2     | 126.200.1.3 | 200  |

## 3.6 配置文件

- AC 1:

```
#
wlan backup-ap enable
#
wlan backup-client enable
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 126.100.1.1 255.255.255.0
vrrp vrid 1 virtual-ip 126.100.1.253
vrrp vrid 1 priority 110
vrrp vrid 1 preempt-mode timer delay 6
#
interface Vlan-interface200
ip address 126.200.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
port hybrid vlan 1 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap testap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1
radio enable
#
wlan mobility-group 1
member ip 126.100.1.2
source ip 126.100.1.1
mobility-group enable
```

```

#
•   AC 2:
#
wlan backup-ap enable
#
wlan backup-client enable
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 126.100.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 126.100.1.253
vrrp vrid 1 preempt-mode timer delay 6
#
interface Vlan-interface200
ip address 126.200.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
port hybrid vlan 1 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap testap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1
radio enable
#
wlan mobility-group 1
member ip 126.100.1.1
source ip 126.100.1.2
mobility-group enable
#

```

• Switch:

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
#
interface GigabitEthernet1/0/4
port link-type access
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“可靠性配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“可靠性命令参考”。

# 无线控制器 IPv6 VRRP 热备管理 AP 的 IPv6 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |    |
|------------------------|----|
| 1 简介.....              | 1  |
| 2 配置前提 .....           | 1  |
| 3 配置举例 .....           | 1  |
| 3.1 组网需求 .....         | 1  |
| 3.2 配置思路 .....         | 1  |
| 3.3 配置注意事项.....        | 2  |
| 3.4 配置步骤 .....         | 2  |
| 3.4.1 AC 1 的配置 .....   | 2  |
| 3.4.2 AC 2 的配置 .....   | 4  |
| 3.4.3 Switch 的配置 ..... | 6  |
| 3.5 验证配置 .....         | 7  |
| 3.6 配置文件 .....         | 9  |
| 4 相关资料 .....           | 12 |



# 1 简介

本文档介绍了无线控制器 VRRP 热备管理 AP 的 IPv6 典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 接入、VRRP 热备等特性。

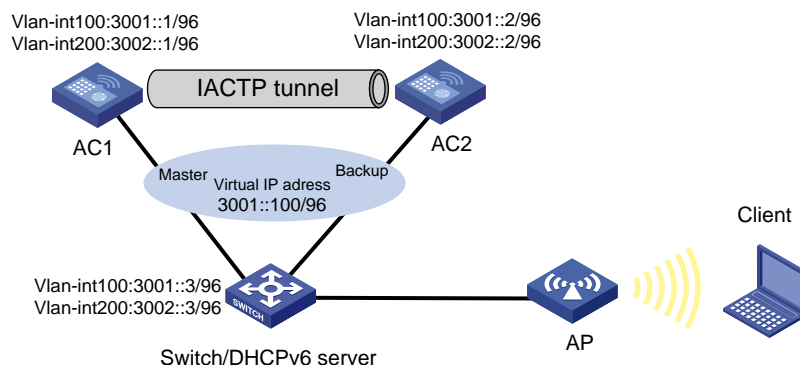
## 3 配置举例

### 3.1 组网需求

如图 1 所示，为了提高网络中 AC 的可靠性，现要求使用 VRRP 热备功能，将 AC 1 和 AC 2 组成一台虚拟 AC，为 Client 提供无线接入服务。具体要求如下：

- AC 1 正常工作的情况下，Client 通过 AC 1 访问网络。
- 当 AC 1 发生故障时，Client 切换至 AC 2 上，保证业务流量在切换过程中不会中断。

图1 VRRP 热备管理 AP 的 IPv6 典型组网图



### 3.2 配置思路

- 为了让 AC 1 成为 VRRP 备份组中的 Master，需要为 AC 1 配置较高的优先级。
- 为了避免 VRRP 备份组中的角色频繁发生变化，可以配置一定的抢占延迟时间。
- 当备份组中的角色发生变化时，为了保证网络流量不会中断，需要在 AC 1 和 AC 2 之间建立 IACTP 隧道，并通过 AP 信息备份以及 Client 备份功能，使 AC 之间可以同步备份 AP 和 Client 的信息。

### 3.3 配置注意事项

- 两台 AC 需保证 WLAN 相关的特性配置一致，否则可能出现备份失败等问题。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 需要确保在完成 VRRP 配置、IACTP 隧道、开启客户端信息备份功能后，再开启 AP 信息备份功能。
- 需要在配置 IACTP 隧道的源 IPv6 地址后才可以开启隧道。

### 3.4 配置步骤

#### 3.4.1 AC 1 的配置

(1) 配置 AC 1 的接口

# 全局使能 IPv6 功能。

```
<AC1> system-view
```

```
[AC1] ipv6
```

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。AC 1 将使用该接口的 IPv6 地址与 AP 建立 LWAPP 隧道，同时用于与 AC 2 建立 VRRP 备份组和 IACTP 隧道。

```
[AC1] vlan 100
```

```
[AC1-vlan100] quit
```

```
[AC1] interface vlan-interface 100
```

```
[AC1-Vlan-interface100] ipv6 address fe80::1 link-local
```

```
[AC1-Vlan-interface100] ipv6 address 3001::1 96
```

```
[AC1-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址。

```
[AC1] vlan 200
```

```
[AC1-vlan200] quit
```

```
[AC1] interface vlan-interface 200
```

```
[AC1-Vlan-interface200] ipv6 address 3002::1 96
```

```
[AC1-Vlan-interface200] quit
```

# 配置 AC 1 与 Switch 相连的 GigabitEthernet1/0/1 接口链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 200 的报文通过。

```
[AC1] interface gigabitethernet 1/0/1
```

```
[AC1-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[AC1-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[AC1-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS 1 接口

```
[AC1] interface wlan-ess 1
```

# 配置 WLAN-ESS 1 接口链路类型为 Hybrid。

```
[AC1-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，允许 VLAN 200 不带 tag 通过。

```
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC1-WLAN-ESS1] mac-vlan enable
```

```
[AC1-WLAN-ESS1] quit
```

## (2) 配置 VRRP 功能

# 创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 3001::100。

```
[AC1] interface vlan-interface 100
```

```
[AC1-Vlan-interface100] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

```
[AC1-Vlan-interface100] vrrp ipv6 vrid 1 virtual-ip 3001::100
```

# 设置 AC 1 在备份组 1 中的优先级为 110。

```
[AC1-Vlan-interface100] vrrp ipv6 vrid 1 priority 110
```

# 设置 AC 1 工作在抢占模式，抢占延迟时间为 6 秒。

```
[AC1-Vlan-interface100] vrrp ipv6 vrid 1 preempt-mode timer delay 6
```

# 配置允许发布 RA 消息。

```
[AC1-Vlan-interface100] undo ipv6 nd ra halt
```

```
[AC1-Vlan-interface100] quit
```

## (3) 配置 IACTP 隧道

# 创建 IACTP 隧道 1，并进入其视图。

```
[AC1] wlan mobility-group 1
```

# 配置 IACTP 隧道 1 的隧道类型为 iactp6。

```
[AC1-wlan-mg-1] mobility-tunnel iactp6
```

# 配置 IACTP 隧道 1 的源 IPv6 地址为 AC 1 的 IPv6 地址 3001::1。

```
[AC1-wlan-mg-1] source ipv6 3001::1
```

# 配置 IACTP 隧道 1 的成员 IPv6 地址为 AC 2 的 IPv6 地址 3001::2。

```
[AC1-wlan-mg-1] member ipv6 3001::2
```

# 开启 IACTP 隧道。

```
[AC1-wlan-mg-1] mobility-group enable
```

```
[AC1-wlan-mg-1] quit
```

# 开启客户端信息备份功能。

```
[AC1] wlan backup-client enable
```

# 设置 AC 1 的备份 AC 为 AC 2。

```
[AC1] wlan backup-ac ipv6 3001::2
```

## (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC1] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC1-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC1-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC1-wlan-st-1] service-template enable
```

```
[AC1-wlan-st-1] quit
```

## (5) 配置 AP

# 创建 AP 的管理模板，名称为 **testap**，型号名称选择 **WA2620E-AGN**。

```
[AC1] wlan ap testap model WA2620E-AGN
```

# 设置 AP 的序列号为 **21023529G007C000020**。

```
[AC1-wlan-ap-testap] serial-id 21023529G007C000020
```

# 进入 **radio 2** 射频视图。

```
[AC1-wlan-ap-testap] radio 2
```

# 将在 **AC** 上配置 **clear** 类型的服务模板 **1** 与射频 **2** 进行关联。

```
[AC1-wlan-ap-testap-radio-2] service-template 1
```

# 使能 AP 的 **radio 2**。

```
[AC1-wlan-ap-testap-radio-2] radio enable
```

```
[AC1-wlan-ap-testap-radio-2] return
```

### 3.4.2 AC 2 的配置

(1) 配置 AC 2 的接口

# 全局使能 **IPv6** 功能。

```
<AC2> system-view
```

```
[AC2] ipv6
```

# 创建 **VLAN 100** 及其对应的 **VLAN** 接口，并为该接口配置 **IPv6** 地址。**AC 2** 将使用该接口的 **IPv6** 地址与 **AP** 建立 **LWAPP** 隧道，同时用于与 **AC 1** 建立 **VRRP** 备份组和 **IACP** 隧道。

```
[AC2] vlan 100
```

```
[AC2-vlan100] quit
```

```
[AC2] interface vlan-interface 100
```

```
[AC2-Vlan-interface100] ipv6 address fe80::2 link-local
```

```
[AC2-Vlan-interface100] ipv6 address 3001::2 96
```

```
[AC2-Vlan-interface100] quit
```

# 创建 **VLAN 200** 作为 **WLAN-ESS** 接口的缺省 **VLAN**，同时作为 **Client** 接入的业务 **VLAN**，并为该接口配置 **IP** 地址。

```
[AC2] vlan 200
```

```
[AC2-vlan200] quit
```

```
[AC2] interface vlan-interface 200
```

```
[AC2-Vlan-interface200] ipv6 address 3002::2 96
```

```
[AC2-Vlan-interface200] quit
```

# 配置 **AC 2** 与 **Switch** 相连的 **GigabitEthernet1/0/1** 接口链路类型为 **Trunk**，**PVID** 为 **100**，允许 **VLAN 100** 和 **VLAN 200** 的报文通过。

```
[AC2] interface gigabitethernet 1/0/1
```

```
[AC2-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[AC2-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[AC2-GigabitEthernet1/0/1] quit
```

# 创建 **WLAN-ESS 1** 接口

```
[AC2] interface wlan-ess 1
```

# 配置 **WLAN-ESS 1** 接口链路类型为 **Hybrid**。

```
[AC2-WLAN-ESS1] port link-type hybrid
```

# 配置当前 **Hybrid** 端口的 **PVID** 为 **VLAN 200**，允许 **VLAN 200** 不带 **tag** 通过。

```
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC2-WLAN-ESS1] mac-vlan enable
[AC2-WLAN-ESS1] quit
```

## (2) 配置 VRRP

# 创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10 和 3001::100，AC 2 在备份组 1 中的优先级缺省值 100。

```
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[AC2-Vlan-interface100] vrrp ipv6 vrid 1 virtual-ip 3001::100
```

# 设置 AC 2 工作在抢占方式，抢占延迟时间为 6 秒。

```
[AC2-Vlan-interface100] vrrp ipv6 vrid 1 preempt-mode timer delay 6
```

# 配置允许发布 RA 消息。

```
[AC2-Vlan-interface100] undo ipv6 nd ra halt
[AC2-Vlan-interface100] quit
```

## (3) 配置 IACTP 隧道

# 创建 IACTP 隧道 1，并进入其视图。

```
[AC2] wlan mobility-group 1
```

# 配置 IACTP 隧道 1 的隧道类型为 iactp6。

```
[AC2-wlan-mg-1] mobility-tunnel iactp6
```

# 配置 IACTP 隧道 1 的源 IPv6 地址为 AC 2 的 IP 地址 3001::2。

```
[AC2-wlan-mg-1] source ipv6 3001::2
```

# 配置配置 IACTP 隧道 1 的成员 IPv6 地址为 AC 1 的 IPv6 地址 3001::1。

```
[AC2-wlan-mg-1] member ipv6 3001::1
```

# 开启 IACTP 隧道。

```
[AC2-wlan-mg-1] mobility-group enable
[AC2-wlan-mg-1] quit
```

# 开启客户端信息备份功能。

```
[AC2] wlan backup-client enable
```

# 设置 AC 2 的备份 AC 为 AC 1。

```
[AC2] wlan backup-ac ipv6 3001::1
```

## (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC2] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC2-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC2-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
```

## (5) 配置 AP

# 创建 AP 的管理模板，名称为 **testap**，型号名称选择 **WA2620E-AGN**。

```
[AC2] wlan ap testap model WA2620E-AGN
```

# 设置 AP 的序列号为 **21023529G007C000020**。

```
[AC2-wlan-ap-testap] serial-id 21023529G007C000020
```

# 进入 **radio 2** 射频视图。

```
[AC2-wlan-ap-testap] radio 2
```

# 将在 **AC** 上配置 **clear** 类型的服务模板 **1** 与射频 **2** 进行关联。

```
[AC2-wlan-ap-testap-radio-2] service-template 1
```

# 使能 AP 的 **radio 2**。

```
[AC2-wlan-ap-testap-radio-2] radio enable
```

```
[AC2-wlan-ap-testap-radio-2] return
```

### 3.4.3 Switch 的配置

# 全局使能 **IPv6** 功能。

```
<Switch> system-view
```

```
[Switch] ipv6
```

# 使能 **DHCPv6** 服务器功能。

```
[Switch] ipv6 dhcp server enable
```

# 创建 **VLAN 100** 和 **VLAN 200**，其中 **VLAN 100** 用于转发 **AC** 和 **AP** 间 **LWAPP** 隧道内的流量，**VLAN 200** 为无线客户端接入的 **VLAN**。

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

# 配置 **Switch** 与 **AC 1** 相连的 **GigabitEthernet1/0/1** 接口属性 **Trunk**，当前 **Trunk** 口的 **PVID** 为 **100**，允许 **VLAN 100** 和 **VLAN 200** 通过。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 **Switch** 与 **AC 2** 相连的 **GigabitEthernet1/0/2** 接口属性 **Trunk**，**PVID** 为 **100**，允许 **VLAN 100** 和 **VLAN 200** 通过。

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

```
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 **Switch** 与 **AP** 相连的 **GigabitEthernet1/0/4** 接口属性为 **Access**，并允许 **VLAN 100** 通过，并使能 **PoE** 功能。

```
[Switch] interface gigabitethernet 1/0/4
```

```
[Switch-GigabitEthernet1/0/4] port link-type access
```

```
[Switch-GigabitEthernet1/0/4] port access vlan 100
```

```
[Switch-GigabitEthernet1/0/4] poe enable
```

```

[Switch-GigabitEthernet1/0/4] quit
# 配置 VLAN 100 接口的 IPv6 地址。
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 3001::3/96
[Switch-Vlan-interface100] quit
# 配置 VLAN 200 接口的 IPv6 地址。
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ipv6 address 3002::3/96
[Switch-Vlan-interface200] quit
# 配置 DHCPv6 地址池 1，用于为 AP 分配 IPv6 地址。
[Switch] ipv6 dhcp pool 1
[Switch-dhcp6-pool-1] network 3001::/96
[Switch-dhcp6-pool-1] quit
[Switch] ipv6 dhcp server forbidden-address 3001::1 3001::2
# 配置在 VLAN 100 接口下引用地址池 1。
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 dhcp server apply pool 1
# 取消 VLAN 100 接口对 RA 消息发布的抑制。配置被管理地址的配置标志位为 1，即主机通过
DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取
除 IPv6 地址以外的其他信息。
[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface100] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface100] undo ipv6 nd ra halt
[Switch-Vlan-interface100] quit
# 配置 DHCPv6 地址池 2，用于为 Client 分配 IPv6 地址。
[Switch] ipv6 dhcp pool 2
[Switch-dhcp6-pool-2] network 3002::/96
[Switch-dhcp6-pool-2] quit
[Switch] ipv6 dhcp server forbidden-address 3002::1 3002::2
# 配置在 VLAN 200 接口下引用地址池 2。
[Switch] interface Vlan-interface 200
[Switch-Vlan-interface200] ipv6 dhcp server apply pool 2
# 取消 VLAN 200 接口下对 RA 消息发布的抑制。配置被管理地址的配置标志位为 1，即主机通过
DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取
除 IPv6 地址以外的其他信息。
[Switch-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface200] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface200] undo ipv6 nd ra halt
[Switch-Vlan-interface200] quit

```

### 3.5 验证配置

- (1) 当 MAC 地址为 3829-5a40-9589 的 Client 通过 SSID 为 service 的无线服务上线时，在 AC 1 上通过 **display wlan ap all** 命令可以查看 AP 和 Client 的信息。

```

<AC1> display wlan ap all
Total Number of APs configured          : 1

```

```

Total Number of configured APs connected : 1
Total Number of auto APs connected      : 0
Total Number of APs connected           : 1
Maximum AP capacity                      : 64
Remaining AP capacity                    : 63

```

#### AP Profiles

```

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
       C = Config, R = Run, KU = KeyUpdate, KC = KeyCfm
       M = Master, B = Backup

```

| AP Name | State Model     | Serial-ID           |
|---------|-----------------|---------------------|
| testap  | R/M WA2620E-AGN | 21023529G007C000020 |

<AC1> display wlan client

```

Total Number of Clients      : 1
Client Information

```

SSID: service

| MAC Address    | User Name | APID/RID | IP Address | IPv6 Address | VLAN |
|----------------|-----------|----------|------------|--------------|------|
| 3829-5a40-9589 | -NA-      | 1 /2     | 0.0.0.0    | -NA-         | 200  |

(2) 此时在 AC 2 上通过 **display wlan ap all** 命令查看到 AP 和 Client 的信息，可以看见 AP 和 Client 信息已经备份到 AC 2。

<AC2> display wlan ap all

```

Total Number of APs configured      : 1
Total Number of configured APs connected : 1
Total Number of auto APs connected   : 0
Total Number of APs connected       : 1
Maximum AP capacity                  : 64
Remaining AP capacity                : 63

```

#### AP Profiles

```

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
       C = Config, R = Run, KU = KeyUpdate, KC = KeyCfm
       M = Master, B = Backup

```

| AP Name | State Model     | Serial-ID           |
|---------|-----------------|---------------------|
| testap  | R/B WA2620E-AGN | 21023529G007C000020 |

<AC2> display wlan client

```

Total Number of Clients      : 1
Client Information

```

SSID: service

| MAC Address | User Name | APID/RID | IP Address | IPv6 Address | VLAN |
|-------------|-----------|----------|------------|--------------|------|
|-------------|-----------|----------|------------|--------------|------|



-----  
3829-5a40-9589 -NA-

1 /2 0.0.0.0

-NA-

200  
-----

## 3.6 配置文件

### • AC 1:

```
#
ipv6
#
wlan backup-ac ipv6 3001::2
#
wlan backup-client enable
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
undo ipv6 nd ra halt
ipv6 address 3001::1/96
ipv6 address FE80::1 link-local
vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
vrrp ipv6 vrid 1 virtual-ip 3001::100
vrrp ipv6 vrid 1 priority 110
vrrp ipv6 vrid 1 preempt-mode timer delay 6
#
interface Vlan-interface200
ipv6 address 3002::1/96
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface WLAN-ESS1
port link-type hybrid
port hybrid vlan 1 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap testap model WA2620E-AGN id 1
```

```

serial-id 21023529G007C000020
radio 1
    radio enable
radio 2
    service-template 1
    radio enable
#
wlan mobility-group 1
    mobility-tunnel iactp6
    member ipv6 3001::2
    source ipv6 3001::1
    mobility-group enable
#
•   AC 2:
#
    ipv6
#
    wlan backup-ac ipv6 3001::1
#
    wlan backup-client enable
#
    vlan 1
#
    vlan 100
#
    vlan 200
#
    wlan service-template 1 clear
        ssid service
        bind WLAN-ESS 1
        service-template enable
#
    interface Vlan-interface100
        undo ipv6 nd ra halt
        ipv6 address 3001::2/96
        ipv6 address FE80::2 link-local
        vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
        vrrp ipv6 vrid 1 virtual-ip 3001::100
        vrrp ipv6 vrid 1 preempt-mode timer delay 6
#
    interface Vlan-interface200
        ipv6 address 3002::2/96
#
    interface GigabitEthernet1/0/1
        port link-type trunk
        port trunk permit vlan 1 100 200
#
    interface WLAN-ESS1

```

```

port link-type hybrid
port hybrid vlan 1 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap testap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio enable
radio 2
service-template 1
radio enable
#
wlan mobility-group 1
mobility-tunnel iactp6
member ipv6 3001::1
source ipv6 3001::2
mobility-group enable
#
• Switch:
#
ipv6
#
ipv6 dhcp server enable
#
ipv6 dhcp server forbidden-address 3001::1 3001::2
ipv6 dhcp server forbidden-address 3002::1 3002::2
#
vlan 1
#
vlan 100
#
vlan 200
#
ipv6 dhcp pool 1
network 3001::/96
#
ipv6 dhcp pool 2
network 3002::/96
#
interface Vlan-interface100
ipv6 dhcp select server
ipv6 dhcp server apply pool 1
ipv6 address 3001::3/96
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#

```

```
interface Vlan-interface200
    ipv6 dhcp select server
    ipv6 dhcp server apply pool 2
    ipv6 address 3002::3/96
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
    port link-type trunk
    port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/4
    port access vlan 100
    poe enable
#
return
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“可靠性配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“可靠性命令参考”。

# H3C 无线控制器 IPv6 无线网络接入配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 2 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 5 |
| 3.5 验证配置 .....         | 5 |
| 3.6 配置文件 .....         | 7 |
| 4 相关资料 .....           | 9 |

# 1 简介

本文介绍了 H3C 无线控制器 IPv6 无线网络接入配置举例。

## 2 配置前提

本文档适用于使用 Comware V5 软件版本的无线控制器和接入点产品，不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 无线接入、WLAN 安全和 DHCPv6 特性。

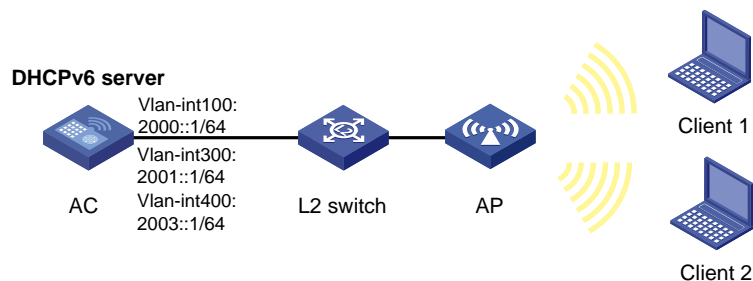
## 3 配置举例

### 3.1 组网需求

如图 1 所示，AP 通过二层交换机与 AC 相连，AC 作为 DHCPv6 服务器为 AP 和 Client 1 动态分配 IPv6 地址，为 Client 2 分配前缀 2003::1/64。要实现无线客户端 Client 1 和 Client 2 通过 AP 连接到 AC 上。

- 无线客户端 Client 1 通过 VLAN 300 接入网络，Client 2 通过 VLAN 400 接入网络。
- 整网使用 IPv6 地址。

图1 IPv6 接入配置组网图



### 3.2 配置思路

- 在 AC 上配置 DHCPv6 服务，使 AP 和无线客户端 Client 都能通过 DHCPv6 server 自动获取 IPv6 地址。
- 在 L2 switch 上开启 PoE 功能，为 AP 设备供电。
- 在 AC 上配置无线服务，确保 Client 可以通过配置的无线服务接入网络。

## 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IPv6 地址。AC 将使用该接口的 IPv6 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
```

# 配置 VLAN 100 的接口 IP 地址为 2000::1/64。

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 address 2000::1/64
```

# 配置 VLAN 接口 100 工作在 DHCPv6 服务器模式，并引用地址池 10，配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```
[AC-Vlan-interface100] ipv6 dhcp server apply pool 10
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 1 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置 VLAN 300 的接口 IP 地址为 2001::1/64。

```
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ipv6 address 2001::1/64
```

# 配置 VLAN 接口 300 工作在 DHCPv6 服务器模式，并引用地址池 30，配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```
[AC-Vlan-interface300] ipv6 dhcp server apply pool 30
[AC-Vlan-interface300] ipv6 nd autoconfig managed-address-flag
[AC-Vlan-interface300] ipv6 nd autoconfig other-flag
[AC-Vlan-interface300] quit
```

# 创建 VLAN 400 作为 Client 2 接入的业务 VLAN。

```
[AC] vlan 400
[AC-vlan400] quit
```

# 配置 VLAN 400 的接口 IP 地址为 2003::1/64。



```

[AC] interface vlan-interface 400
[AC-Vlan-interface400] ipv6 address 2003::1/64
# 配置 VLAN 接口 400 工作在 DHCPv6 服务器模式，并引用地址池 40。
[AC-Vlan-interface400] ipv6 dhcp server apply pool 40
[AC-Vlan-interface400] quit
# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，禁止 VLAN1 通过，配置 PVID 为 100，允许 VLAN 100、VLAN 300 和 VLAN 400 通过。
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300 400
[AC-GigabitEthernet1/0/1] quit
(2) 配置 DHCPv6
# 在 AC 上开启 IPv6 报文转发及 DHCPv6 服务器功能。
[AC] ipv6
[AC] ipv6 dhcp server enable
# 配置 DHCPv6 地址池 10 为 AP 动态分配的网段为 2000::0/64。
[AC] ipv6 dhcp pool 10
[AC-dhcp6-pool-10] network 2000::0/64
[AC-dhcp6-pool-10] quit
# 配置 DHCPv6 地址池 30 为 Client 动态分配的网段为 2001::0/64。
[AC] ipv6 dhcp pool 30
[AC-dhcp6-pool-30] network 2001::0/64
[AC-dhcp6-pool-30] quit
# 配置前缀池 1，包含的前缀为 2003::0/64，分配的前缀长度为 64。
[AC] ipv6 dhcp prefix-pool 1 prefix 2003::0/64 assign-len 64
# 配置 DHCPv6 地址池 40 引用已存在的前缀池 1。
[AC] ipv6 dhcp pool 40
[AC-dhcp6-pool-40] prefix-pool 1
[AC-dhcp6-pool-40] quit
(3) 配置 WLAN-ESS 接口
# 创建 WLAN-ESS1 接口。
[AC] interface wlan-ess 1
# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。
[AC-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200、VLAN 300 和 VLAN 400 不带 tag 通过。
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 300 400 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
# 使能 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
(4) 配置无线服务

```

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

# 创建 clear 类型的服务模板 2。

```
[AC] wlan service-template 2 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-2] ssid service2
```

# 将 WLAN-ESS1 接口绑定到服务模板 2。

```
[AC-wlan-st-2] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-2] service-template enable
```

```
[AC-wlan-st-2] quit
```

#### (5) 配置射频接口并绑定服务模板

# 创建 AP 的管理模板，名称为 officeap，型号名称这里选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 officeap 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-officeap] radio 1
```

# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 1 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 300。

```
[AC-wlan-ap-officeap-radio-1] service-template 1 vlan-id 300
```

# 使能 officeap 的 radio 1。

```
[AC-wlan-ap-officeap-radio-1] radio enable
```

```
[AC-wlan-ap-officeap-radio-1] quit
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 2 与射频 2 进行关联，同时设置绑定到该射频的 VLAN 为 VLAN 400。

```
[AC-wlan-ap-officeap-radio-2] service-template 2 vlan-id 400
```

# 使能 officeap 的 radio 2。

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

```
[AC-wlan-ap-officeap] quit
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100、VLAN 300 和 VLAN 400，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 和 VLAN 400 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] vlan 400
[Switch-vlan400] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止 VLAN 1 通过，并允许 VLAN 100、VLAN 300 和 VLAN 400 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300 400
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

## 3.5 验证配置

# 通过命令 **display wlan client** 可以看到 Client 1 和 Client 2 已经接入无线服务。

```
[AC] display wlan client
Total Number of Clients          : 2
Client Information
SSID: service
-----
MAC Address      User Name      APID/RID IP Address      VLAN
-----
0024-d774-6edc -NA-          1 /1      2001::2          300
0024-d774-6edd -NA-          1 /2      2003::2          400
-----
```

# 通过命令 **display wlan client verbose** 可以看到 Client 1 和 Client 2 上线的详细信息。

```
[AC] display wlan client verbose
Total Number of Clients          : 2
Client Information
-----
MAC Address          : 0024-d774-6edc
User Name            : -NA-
```

|                                   |                                             |
|-----------------------------------|---------------------------------------------|
| IP Address                        | : 2001::2                                   |
| AID                               | : 1                                         |
| AP Name                           | : officeap                                  |
| Radio Id                          | : 1                                         |
| Antenna Id                        | : 0                                         |
| Service Template Number           | : 1                                         |
| SSID                              | : service                                   |
| BSSID                             | : 80f6-2ee1-44b0                            |
| Port                              | : WLAN-DBSS1:0                              |
| VLAN                              | : 300                                       |
| State                             | : Running                                   |
| Power Save Mode                   | : Active                                    |
| Wireless Mode                     | : 11gn                                      |
| Channel Band-width                | : 20MHz                                     |
| SM Power Save Enable              | : Disabled                                  |
| Short GI for 20MHz                | : Supported                                 |
| Short GI for 40MHz                | : Not Supported                             |
| STBC TX capability                | : Not Supported                             |
| STBC RX capability                | : Supported                                 |
| Support MCS Set                   | : 0,1,2,3,4,5,6,7,8,9,<br>10,11,12,13,14,15 |
| QoS Mode                          | : WMM                                       |
| Listen Interval (Beacon Interval) | : 10                                        |
| RSSI                              | : 48                                        |
| Rx/Tx Rate                        | : 6/117                                     |
| Client Type                       | : PRE-RSNA                                  |
| Authentication Method             | : Open System                               |
| Authentication Mode               | : Central                                   |
| AKM Method                        | : None                                      |
| 4-Way Handshake State             | : -NA-                                      |
| Group Key State                   | : -NA-                                      |
| Encryption Cipher                 | : Clear                                     |
| Roam Status                       | : Normal                                    |
| Roam Count                        | : 0                                         |
| Up Time (hh:mm:ss)                | : 00:02:02                                  |

---

|                         |                  |
|-------------------------|------------------|
| MAC Address             | : 0024-d774-6edd |
| User Name               | : -NA-           |
| IP Address              | : 2003::2        |
| AID                     | : 1              |
| AP Name                 | : officeap       |
| Radio Id                | : 2              |
| Antenna Id              | : 0              |
| Service Template Number | : 2              |
| SSID                    | : servicel       |
| BSSID                   | : 80f6-2ee1-44b1 |
| Port                    | : WLAN-DBSS1:0   |
| VLAN                    | : 400            |

```

State : Running
Power Save Mode : Active
Wireless Mode : 11gn
Channel Band-width : 20MHz
SM Power Save Enable : Disabled
Short GI for 20MHz : Supported
Short GI for 40MHz : Not Supported
STBC TX capability : Not Supported
STBC RX capability : Supported
Support MCS Set : 0,1,2,3,4,5,6,7,8,9,
                  10,11,12,13,14,15

QoS Mode : WMM
Listen Interval (Beacon Interval) : 10
RSSI : 48
Rx/Tx Rate : 6/117
Client Type : PRE-RSNA
Authentication Method : Open System
Authentication Mode : Central
AKM Method : None
4-Way Handshake State : -NA-
Group Key State : -NA-
Encryption Cipher : Clear
Roam Status : Normal
Roam Count : 0
Up Time (hh:mm:ss) : 00:02:02
-----

```

## 3.6 配置文件

- AC

```

#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
ipv6 dhcp pool vlan100
    network 2000::0 64
#
ipv6 dhcp pool vlan300
    network 2001::0 64
#
ipv6 dhcp pool vlan400
    network 2003::0 64
#

```

```

wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable
#
wlan service-template 2 clear
  ssid service1
  bind WLAN-ESS 1
  service-template enable
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk pvid vlan 100
  port trunk permit vlan 100 300 400
#
interface Vlan-interface100
  ipv6 dhcp server apply pool 10
  ipv6 nd autoconfig managed-address-flag
  ipv6 nd autoconfig other-flag
  ipv6 address 2000::1/64
#
interface Vlan-interface300
  ipv6 dhcp server apply pool 30
  ipv6 nd autoconfig managed-address-flag
  ipv6 nd autoconfig other-flag
  ipv6 address 2001::1/64
#
interface Vlan-interface400
  ipv6 dhcp server apply pool 40
  ipv6 address 2003::1/64
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 300 400 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
    service-template 1 vlan-id 300
    radio enable
  radio 2
    service-template 2 vlan-id 400
    radio enable
#

```

```
ipv6
#
ipv6 dhcpv6 server enable
#
• Switch:
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 300 400
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 无线控制器通过认证服务器动态授权无线终端接入 VLAN 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

|                          |    |
|--------------------------|----|
| 1 简介.....                | 1  |
| 2 配置前提 .....             | 1  |
| 3 配置举例 .....             | 1  |
| 3.1 组网需求 .....           | 1  |
| 3.2 配置注意事项.....          | 1  |
| 3.3 配置步骤.....            | 2  |
| 3.3.1 AC 的配置 .....       | 2  |
| 3.3.2 Switch 的配置 .....   | 4  |
| 3.3.3 RADIUS 服务器配置 ..... | 6  |
| 3.4 验证配置 .....           | 9  |
| 3.5 配置文件 .....           | 10 |
| 4 相关资料 .....             | 12 |

# 1 简介

本文档介绍了无线控制器通过认证服务器动态授权无线终端接入 VLAN 典型配置案例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

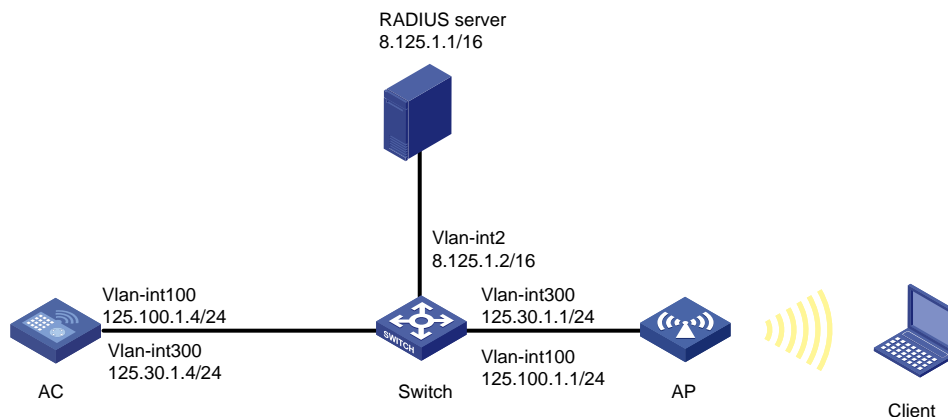
本文档假设您已了解 802.1X 特性。

## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，在无线网络环境中部署了 RADIUS 服务器，现要求使用 RADIUS 服务器对无线客户端进行 802.1X 认证，并对认证通过的客户端下发授权 VLAN 300。

图1 授权 VLAN 下发典型配置组网图



### 3.2 配置注意事项

- 开启无线侧的端口安全功能时，请确保该端口的 802.1X 功能或 MAC 地址认证功能处于关闭状态。
- 关闭在线用户握手功能，以避免不支持在线握手功能的客户端被强制下线。
- # 关闭 802.1X 的组播触发功能，以节省无线的通信带宽。
- RADIUS 服务器授权下发的 VLAN 必须是 AC 设备上已经配置的 VLAN，否则 802.1X 无法认证成功。

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应, AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口, 并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 125.100.1.4 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN, 且 RADIUS 服务器会下发 VLAN 300 作为授权 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置 VLAN 300 的接口 IP 地址为 125.30.1.4/24。

```
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 125.30.1.4 24
[AC-Vlan-interface300] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk, 配置 PVID 为 100, 禁止 VLAN 1 通过, 允许 VLAN 100 和 VLAN 300 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 802.1X 认证

# 全局模式下使能端口安全。

```
[AC] port-security enable
```

# 选择 802.1X 认证方式为 EAP。

```
[AC] dot1x authentication-method eap
```

#### (3) 配置认证策略

# 创建 RADIUS 方案 office 并进入其视图。

```
[AC] radius scheme office
```

# 配置 RADIUS 方案服务类型为扩展型。

```
[AC-radius-office] server-type extended
```

```
# 设置主认证 RADIUS 服务器的 IP 地址 8.125.1.1。
[AC-radius-office] primary authentication 8.125.1.1
# 设置主计费 RADIUS 服务器的 IP 地址 8.125.1.1。
[AC-radius-office] primary accounting 8.125.1.1
# 设置系统与认证 RADIUS 服务器交互报文时的共享密钥为 123456。
[AC-radius-office] key authentication 123456
# 设置系统与计费 RADIUS 服务器交互报文时的共享密钥为 123456。
[AC-radius-office] key accounting 123456
# 认证时用户名不携带域。
[AC-radius-office] user-name-format without-domain
# 设置设备发送 RADIUS 报文时使用的源 IP 地址 125.100.1.4。
[AC-radius-radius] nas-ip 125.100.1.4
[AC-radius-radius] quit
```

#### (4) 配置认证域

```
# 创建 office 域并进入其视图。
[AC] domain office
# 为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 office。
[AC-isp-office] authentication lan-access radius-scheme office
# 为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 office。
[AC-isp-office] authorization lan-access radius-scheme office
# 为 lan-access 用户配置计费为 none，不计费。
[AC-isp-office] accounting lan-access none
[AC-isp-office] quit
```

#### (5) 配置无线接口

```
# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
# 在 Hybrid 端口上使能 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
# 在 WLAN-ESS1 口上配置端口安全，安全模式为 userlogin-secure-ext。
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
# 在接口 WLAN-ESS1 下使能 11key 类型的密钥协商功能。
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 关闭在线用户握手功能。
[AC-WLAN-ESS1] undo dot1x handshake
# 关闭 802.1X 的组播触发功能。
[AC-WLAN-ESS1] undo dot1x multicast-trigger
# 在 WLAN-ESS1 端口上指定 802.1X 认证的强制认证域为 office。
[AC-WLAN-ESS1] dot1x mandatory-domain office
```

```

[AC-WLAN-ESS1] quit
(6) 配置无线服务
# 创建 crypto 类型的服务模板 1。
[AC] wlan service-template 1 crypto
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 配置加密套件为 CCMP。
[AC-wlan-st-1] cipher-suite ccmp
# 配置安全信息元素为 RSN。
[AC-wlan-st-1] security-ie rsn
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(7) 配置射频接口并绑定服务模板
# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。
[AC] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-officeap-radio-2] service-template 1
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
# 将 AC 的默认路由指向交换机，地址为 125.100.1.1
[AC] ip route-static 0.0.0.0 0.0.0.0 125.100.1.1

```

### 3.3.2 Switch 的配置

# 创建 VLAN 2、VLAN 100 和 VLAN 300，其中 VLAN 2 用于连接 RADIUS 服务器，VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN。

```

<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit

```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止 VLAN 1 通过，允许 VLAN 2、100 和 300 通过。

```

[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 2 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并加入 VLAN 100。
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 RADIUS 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 2
通过。
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit
# 配置 VLAN 2 的接口地址为 8.125.1.2/16，用于连接 RADIUS 服务器。
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 8.125.1.2 16
[Switch-Vlan-interface2] quit
# 配置 VLAN 100 的接口地址为 125.100.1.1/24
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 125.100.1.1 24
[Switch-Vlan-interface100] quit
# 配置 VLAN 300 的接口地址为 125.30.1.1/24
[Switch] interface vlan-interface 300
[Switch-Vlan-interface300] ip address 125.30.1.1 24
[Switch-Vlan-interface300] quit
# 配置 Switch 使能 DHCP 服务。
[Switch] dhcp enable
# 创建名为 vlan100 的 DHCP 地址池，配置地址池范围为 125.100.1.0~125.100.1.250，网关地址
为 125.100.1.1，为 AP 分配 IP 地址。
[Switch] dhcp server ip-pool vlan100 extended
[Switch-dhcp-pool-vlan100] network ip range 125.100.1.0 125.100.1.250
[Switch-dhcp-pool-vlan100] network mask 255.255.255.0
[Switch-dhcp-pool-vlan100] gateway-list 125.100.1.1
[Switch-dhcp-pool-vlan100] quit
# 创建名为 vlan300 的 DHCP 地址池，配置地址池范围为 125.30.1.0~125.30.1.250，网关地址为
125.30.1.1，为 Client 分配 IP 地址。
[Switch] dhcp server ip-pool vlan300 extended
[Switch-dhcp-pool-vlan300] network ip range 125.30.1.0 125.30.1.250
[Switch-dhcp-pool-vlan300] network mask 255.255.255.0
[Switch-dhcp-pool-vlan300] gateway-list 125.30.1.1

```

[Switch-dhcp-pool-vlan300] quit

### 3.3.3 RADIUS 服务器配置



#### 说明

下面以 iMC 作为 RADIUS 服务为例（使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)），说明 RADIUS 服务器的配置。

# 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，单击“增加”按钮，进入“增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C（General）”；
- 选择手工增加接入设备，添加 IP 地址为 125.100.1.4 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

|        |              |          |         |
|--------|--------------|----------|---------|
| 认证端口 * | 1812         | 计费端口 *   | 1813    |
| 组网方式   | 不启用混合组网      | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 接入设备分组   | 无       |
| 共享密钥 * |              | 确认共享密钥 * |         |
| 业务分组   | 未分组          |          |         |

| 设备名称 | 设备IP地址      | 设备型号 | 备注 | 删除 |
|------|-------------|------|----|----|
|      | 125.100.1.4 |      |    |    |

共有1条记录。

确定 取消

# 配置接入策略。

选择“用户”页签，单击导航树中的[用户/接入策略管理/接入策略管理]菜单项，单击“增加”按钮进入“增加接入策略页面”，创建一条接入策略。

- 接入策略名输入“802.1x”。
- 证书认证选择“EAP 证书认证”。
- 证书认证类型选择“EAP-PEAP 认证”。
- 认证证书子类型选择“MS-CHAPV2 认证”。
- 下发 VLAN 输入授权下发的 VLAN “300”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 配置接入策略

用户 > 接入策略管理 > 接入策略管理 > 添加接入策略

基本信息

接入策略名 \* 802.1x

业务分组 \* 未分组

描述

授权信息

接入时段 无

下行速率(Kbps)

上行速率(Kbps)

优先级

分配IP地址 \* 否

启用RSA认证

证书认证 ☐ 不使用 ☒ EAP证书认证 ☐ WAPI证书认证

认证证书类型 EAP-PEAP认证

认证证书子类型 MS-CHAPV2认证

下发VLAN 300

☐ 下发User Profile

☐ 下发ACL

下发用户组

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定 QinQ VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定MSI号码

☐ 绑定计算机名称

☐ 计算机绑定策略

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端键盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 启用iNode客户端

☐ 禁用Windows设备解客户端

☐ 禁用LinuxMacOS设备解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔(分钟) 30

自动重连次数 3

连接处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务

☐ 禁止配置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止接收MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMware NAT服务

☐ 禁用VMware USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式 ☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定 取消

- # 增加接入服务配置。
- 选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，单击“增加”按钮，创建一条接入服务。
- 服务名输入“802.1x”。
  - 缺省接入策略选择之前创建的策略“802.1x”。
  - 其它参数采用缺省值，并单击<确定>按钮完成操作。



图4 配置接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

| 基本信息                                      |                                        |            |          |
|-------------------------------------------|----------------------------------------|------------|----------|
| 服务名 *                                     | 802.1x                                 | 服务后缀       |          |
| 业务分组 *                                    | 未分组                                    | 缺省接入策略 *   | 802.1x ? |
| 缺省安全策略 *                                  | 不使用                                    | 缺省内网外联配置 * | 不使用      |
| 缺省私有属性下发策略 *                              | 不使用 ?                                  |            |          |
| 缺省BYOD页面 *                                | PC - 缺省页面 (PC                          |            |          |
| 服务描述                                      |                                        |            |          |
| <input checked="" type="checkbox"/> 可申请 ? | <input type="checkbox"/> Portal无感知认证 ? |            |          |

| 接入场景列表      |      |      |          |        |        |
|-------------|------|------|----------|--------|--------|
| 名称          | 接入策略 | 安全策略 | 私有属性下发策略 | 内网外联配置 | BYOD页面 |
| 未找到符合条件的记录。 |      |      |          |        |        |

确定 取消

# 增加用户配置。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，单击“增加”按钮，进入“增加接入用户”界面，增加一个接入用户。

- 单击“增加用户”。
- 用户姓名输入“lw”。
- 证件号码输入“000”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 增加用户配置

用户 > 接入用户 > 增加接入用户

接入用户

增加用户

用户姓名 \* 选择 增加用户

帐号 \*

☐ 桥开户用户 ☐ 缺省BYOD用户 ☐ 主机名用户 ☐ 快速认证用户

密码 \*

☒ 允许用户修改密码

生效时间

最大闲置时长(分钟)

Portal无感知认证最大绑定数

登录提示信息

接入服务

服务名

☐ 802.1x

接入设备绑定信息

设备序列号

外层VLAN ID

端口号

分配IP地址

增加用户 - Mozilla Firefox

8.125.1.1/fmc/usr/user/addUserPopUpContent.xhtml

增加用户

基本信息

用户姓名 \* lw 证件号码 \* 000 检查是否可用

通讯地址

电子邮件 ? 用户分组 \* 未分组

确定 取消

# 增加接入用户配置。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，单击“增加”按钮，增加一个接入用户。

- 单击“选择”，在页面中选择之前创建的用户“lw”。
- 账号名输入“lw”。
- 密码与密码确认输入“123456”。
- 选择服务名“802.1x”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加接入用户配置

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

lw

选择

增加用户

帐号名 \*

lw

☐ 拨开用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

时

失效时间

时

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                        | 服务后缀 | 状态  | 分配IP地址 |
|--------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> 802.1x |      | 可申请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

无线SSID

VLAN ID/内层VLAN ID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

MAC地址

IP地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

### 3.4 验证配置

- (1) Client 通过 802.1X 认证上线后，执行 **display connection** 命令，查看 802.1X 用户上线后的基本信息。观察上线信息的 Index，本例中 Index 值为 15。

```
<AC> display connection
Index=15 ,Username=lw@office
MAC=00-24-01-EB-FA-EE
IP=N/A
```

```
IPv6=N/A
Online=00h02m34s
Total 1 connection(s) matched.
```

- (2) 通过执行 **display connection** 命令得到 Client 的 Index 为 15, 执行 **display connection ucibindex 15** 命令, 得到 Client 通过 802.1X 认证后的详细信息。如阴影部分显示, 授权 VLAN 为 300。RADIUS 服务器下发授权 VLAN 成功。

```
<AC> display connection ucibindex 15
Index=15 , Username=lw@office
MAC=00-24-01-EB-FA-EE
IP=N/A
IPv6=N/A
Access=8021X , AuthMethod=EAP
Port Type=Wireless-802.11, Port Name=WLAN-DBSS1:0
Initial VLAN=200, Authorization VLAN=300
ACL Group=Disable
User Profile=N/A
CAR=Disable
Traffic Statistic:
    InputOctets    =11348      OutputOctets    =7785
    InputGigawords=0          OutputGigawords=0
Priority=Disable
SessionTimeout=N/A, Terminate-Action=N/A
Start=2013-11-20 16:57:38 ,Current=2013-11-20 16:58:33 ,Online=00h00m55s
Total 1 connection matched.
```

## 3.5 配置文件

- AC:

```
#
port-security enable
#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
server-type extended
primary authentication 8.125.1.1
primary accounting 8.125.1.1
key authentication cipher $c$3$EnNB6wxpjYSAJMiU2aaeNArZaBzSA13G5A==
key accounting cipher $c$3$o9Wa5f+anDJ56GonM91E7c8otvLF06HKGA==
user-name-format without-domain
nas-ip 125.100.1.4
#
```

```

domain office
 authentication lan-access radius-scheme office
 authorization lan-access radius-scheme office
 accounting lan-access none
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
wlan service-template 1 crypto
 ssid service
 bind WLAN-ESS 1
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk pvid vlan 100
 port trunk permit vlan 100 300
#
interface Vlan-interface100
 ip address 125.100.1.4 255.255.255.0
#
interface Vlan-interface300
 ip address 125.30.1.4 255.255.255.0
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 200 untagged
 port hybrid pvid vlan 200
 mac-vlan enable
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain office
 undo dot1x multicast-trigger
#
wlan ap officeap model WA2620E-AGN id 1
 serial-id 21023529G007C000020
 radio 1
 radio 2
 service-template 1
 radio enable
#
ip route-static 0.0.0.0 0.0.0.0 125.100.1.1

```

```

#
•   Switch:
#
vlan 2
#
vlan 100
#
vlan 300
#
dhcp server ip-pool vlan100 extended
    network ip range 125.100.1.0 128.100.1.250
    network mask 255.255.255.0
    gateway-list 125.100.1.4
#
dhcp server ip-pool vlan300 extended
    network ip range 125.30.1.0 128.30.1.250
    network mask 255.255.255.0
    gateway-list 125.30.1.4
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 2 100 300
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
    port access vlan 100
    poe enable
#
interface GigabitEthernet1/0/2
    port access vlan 2
    poe enable
#
interface Vlan-interface2
    ip address 8.125.1.2 255.255.0.0
#
interface Vlan-interface100
    ip address 125.100.1.1 255.255.255.0
#
interface Vlan-interface300
    ip address 125.30.1.1 255.255.255.0
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。

# 无线终端策略转发典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                           |    |
|---------------------------|----|
| 1 简介.....                 | 1  |
| 2 配置前提 .....              | 1  |
| 3 配置举例 .....              | 1  |
| 3.1 组网需求 .....            | 1  |
| 3.2 配置思路 .....            | 2  |
| 3.3 配置注意事项.....           | 2  |
| 3.4 配置步骤 .....            | 2  |
| 3.4.1 apcfg.txt 配置文件..... | 2  |
| 3.4.2 AC 的配置 .....        | 2  |
| 3.4.3 Switch 的配置 .....    | 5  |
| 3.4.4 配置 iMC .....        | 6  |
| 3.5 验证配置 .....            | 10 |
| 3.6 配置文件 .....            | 11 |
| 4 相关资料 .....              | 14 |



# 1 简介

本文档介绍了 WLAN 的策略转发典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 的集中式转发、本地转发和策略转发特性。

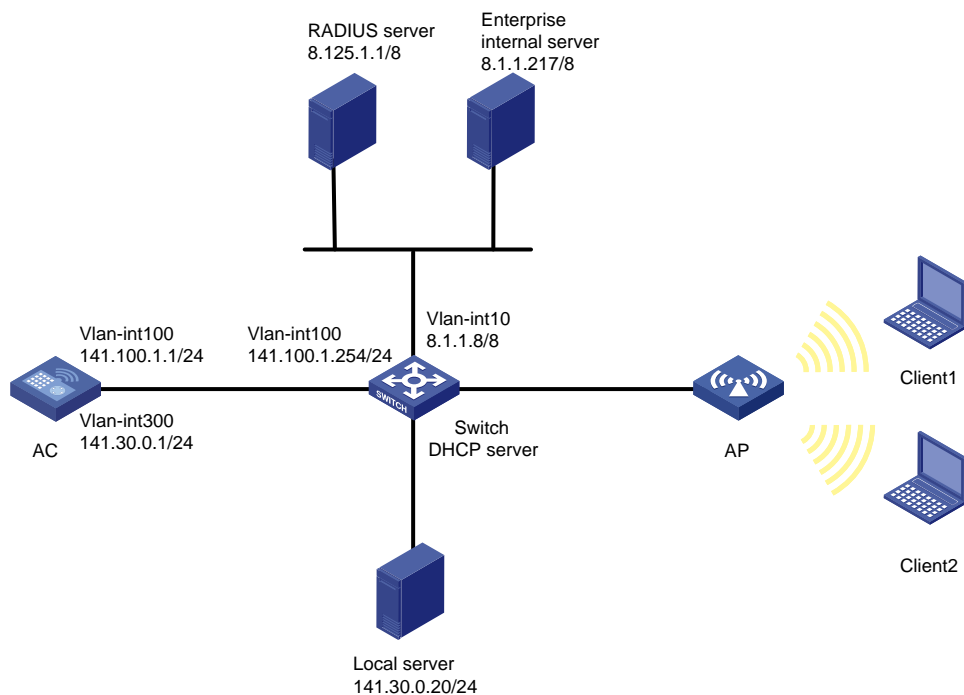
## 3 配置举例

### 3.1 组网需求

如图 1 所示，无线客户端通过 AP 接入 AC；无线客户端 Client 1、Client 2 和 AP 通过 DHCP server 自动获取 IP 地址；Client 1、Client 2 通过 RADIUS 服务器进行 802.1X 认证。现要求通过配置策略转发实现：

- Client 访问本地服务器的流量采用本地转发。
- Client 访问企业网络服务器的流量采用集中转发。

图1 策略转发组网图



## 3.2 配置思路

将转发策略应用到 **User Profile** 上，对匹配转发策略中 **ACL** 的报文进行分类，并采用对应的转发策略进行转发。

## 3.3 配置注意事项

配置 **AP** 的序列号时请确保该序列号与 **AP** 唯一对应，**AP** 的序列号可以通过 **AP** 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 apcfg.txt 配置文件

```
# 编辑 AP 的配置文件 apcfg.txt。
system-view
interface GigabitEthernet 1/0/1
    port link-type trunk
    port trunk permit vlan all
acl number 3000
    rule 0 permit ip destination 141.30.1.20 0
acl number 3001
    rule 0 permit ip destination 8.1.1.217 0
user-profile user
wlan forwarding-policy policy1
user-profile user enable
```

### 3.4.2 AC 的配置

#### (1) 配置 AC 的接口

# 创建 **VLAN 100** 及其对应的 **VLAN** 接口，并为该接口配置 **IP** 地址。**AC** 将使用该接口的 **IP** 地址与 **AP** 建立 **LWAPP** 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
# 配置 VLAN 100 的接口 IP 地址为 141.100.1.1/24。
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 141.100.1.1 255.255.255.0
[AC-Vlan-interface100] quit
```

# 创建 **VLAN 200** 作为 **ESS** 接口的缺省 **VLAN**。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 **VLAN 300** 作为 **Client** 接入的业务 **VLAN**。

```
[AC] vlan 300
[AC-vlan300] quit
```

# 配置 **VLAN 300** 的接口 **IP** 地址为 **141.30.0.1/24**。

```
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 141.30.0.1 255.255.255.0
[AC-Vlan-interface300] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的属性配置为 Trunk, 禁止 VLAN1 通过, 允许 VLAN 100 和 VLAN 300 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置 DHCP

# 在 AC 上开启 DHCP 服务。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 vlan100 为 AP 动态分配的网段为 141.100.1.0/24, 网关地址为 141.100.1.1。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 141.100.1.0 24
[AC-dhcp-pool-vlan100] gateway-list 141.100.1.1
[AC-dhcp-pool-vlan100] quit
```

# 配置 DHCP 地址池 vlan300 为 Client 动态分配的网段为 141.30.0.0/24, 网关地址为 141.30.0.1。

```
[AC] dhcp server ip-pool vlan300
[AC-dhcp-pool-vlan300] network 141.30.0.0 24
[AC-dhcp-pool-vlan300] gateway-list 141.30.0.1
[AC-dhcp-pool-vlan300] quit
```

## (3) 配置认证域

# 创建 office1 域并进入其视图。

```
[AC] domain office1
```

# 在 ISP 域 office1 下, 为 lan-access 用户配置认证、授权方案为 RADIUS 方案, 方案名为 office1。

```
[AC-isp-office1] authentication lan-access radius-scheme office1
[AC-isp-office1] authorization lan-access radius-scheme office1
```

# 在 ISP 域 office1 下, 为 lan-access 用户配置计费方法为 none。

```
[AC-isp-office1] accounting lan-access none
[AC-isp-office1] quit
```

## (4) 配置 WLAN-ESS 接口

# 创建 WLAN-ESS1 接口, 并配置 802.1X 用户的强制认证域为 office1, 链路类型为 Hybrid。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] dot1x mandatory-domain office1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置 WLAN-ESS1 接口的 PVID 为 200, 禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 开启 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

# 开启 802.1X 的端口安全模式。

```
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
```

# 开启 11key 类型的密钥协商功能。

```
[AC-WLAN-ESS1] port-security tx-key-type 11key
```

# 关闭 802.1X 的组播触发功能，以节省无线的通信带宽。

```
[AC-WLAN-ESS1] undo dot1x multicast-trigger
```

# 关闭在线用户握手功能，以避免不支持在线握手功能的客户端被强制下线。

```
[AC-WLAN-ESS1] undo dot1x handshake
```

```
[AC-WLAN-ESS1] quit
```

#### (5) 配置认证策略

# 在 AC 上创建 RADIUS 方案 office1 并进入其视图。

```
[AC] radius scheme office1
```

# 设置主认证、计费 RADIUS 服务器的 IP 地址 8.1.1.5。

```
[AC-radius-office1] primary authentication 8.1.1.5
```

```
[AC-radius-office1] primary accounting 8.1.1.5
```

# 设置系统与认证、计费 RADIUS 服务器交互报文时的共享密钥为 123456。

```
[AC-radius-office1] key authentication simple 123456
```

```
[AC-radius-office1] key accounting simple 123456
```

# 指定发送给 RADIUS 方案 office1 中 RADIUS 服务器的用户名不得携带域名。

```
[AC-radius-office1] user-name-format without-domain
```

```
[AC-radius-office1] quit
```

# 全局使能 802.1X，并设置 802.1X 用户的认证方式为 EAP。

```
[AC] port-security enable
```

```
[AC] dot1x authentication-method eap
```

#### (6) 配置转发策略

# 创建转发策略 policy1，并配置转发规则，对匹配 ACL 3000 的报文进行本地转发，对于匹配 ACL3001 的报文进行集中转发。

```
[AC] wlan forwarding-policy policy1
```

```
[AC-wlan-fp-policy1] classifier acl 3000 behavior local
```

```
[AC-wlan-fp-policy1] classifier acl 3001 behavior remote
```

```
[AC-wlan-fp-policy1] quit
```

#### (7) 配置无线服务

# 创建服务模板 1（加密类型服务模板）。

```
[AC] wlan service-template 1 crypto
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 配置加密方式为 AES-CCMP。

```
[AC-wlan-st-1] cipher-suite ccmp
```

```
[AC-wlan-st-1] security-ie rsn
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

#### (8) 配置射频接口并绑定服务模板

```

# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。
[AC] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的服务模板 1 与射频 2 进行关联，并将服务模板 1 绑定到 VLAN 300。
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 officeap 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
# 在 AC 上通过 map-configuration 命令将配置文件 apcfg.txt 下发到 officeap。
[AC-wlan-ap-officeap] map-configuration apcfg.txt
[AC-wlan-ap-officeap] quit
(9) 配置 User Profile
# 创建名称为 user 的 User Profile 并开启。
[AC] user-profile user
[AC] user-profile user enable
(10) 配置 AC 的静态路由
# 配置静态路由，其目的地址为 8.0.0.0/8，指定下一跳为 141.100.1.254。
[AC] ip route-static 8.0.0.0 255.0.0.0 141.100.1.254

```

### 3.4.3 Switch 的配置

```

# 创建 VLAN 10、VLAN 100 和 VLAN 300，其中 VLAN 10 用于连接 RADIUS 服务器和 Enterprise
internal server，VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户
接入的 VLAN。
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 口的 PVID 为
100，允许 VLAN 10、100、300 通过。
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 10 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，当前 Access 口允许
VLAN100 通过。
[Switch] interface gigabitethernet1/0/2

```

```

[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 RADIUS 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access，当前 Access
口允许 VLAN 2 通过。
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit
# 配置 Switch 与 Enterprise internal server 相连的 GigabitEthernet1/0/4 接口属性为 Access，当前
Access 口允许 VLAN 2 通过。
[Switch] interface gigabitethernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 2
[Switch-GigabitEthernet1/0/4] quit
# 配置 Switch 与 Local server 相连的 GigabitEthernet1/0/5 接口属性为 Access，当前 Access 口允
许 VLAN 300 通过。
[Switch] interface gigabitethernet1/0/5
[Switch-GigabitEthernet1/0/5] port link-type access
[Switch-GigabitEthernet1/0/5] port access vlan 300
[Switch-GigabitEthernet1/0/5] quit
# 配置 VLAN 10 的接口地址为 8.1.1.8/8，用于连接 RADIUS 服务器和 Enterprise internal server。
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 8.1.1.8 8
[Switch-Vlan-interface10] quit
# 配置 VLAN 100 的接口地址为 141.100.1.254/24
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 141.100.1.254 255.255.255.0
[Switch-Vlan-interface100] quit

```

### 3.4.4 配置 iMC



说明

下面以 iMC 作为 RADIUS 服务为例（使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)），说明 RADIUS 服务器的配置。

# 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，单击“增加”按钮，进入“增加接入设备”页面，单击<手工增加>按钮，进入“手工增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”；

- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 141.100.1.1 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

| 接入配置   |              |          |         |
|--------|--------------|----------|---------|
| 认证端口 * | 1812         | 计费端口 *   | 1813    |
| 组网方式   | 不启用混合组网      | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 接入设备分组   | 无       |
| 共享密钥 * | *****        | 确认共享密钥 * | *****   |
| 业务分组   | 未分组          |          |         |

| 设备列表                                                         |             |      |    |    |
|--------------------------------------------------------------|-------------|------|----|----|
| <a href="#">选择</a> <a href="#">手工增加</a> <a href="#">全部清除</a> |             |      |    |    |
| 设备名称                                                         | 设备IP地址      | 设备型号 | 备注 | 删除 |
|                                                              | 141.100.1.1 |      |    |    |

共有1条记录。

[确定](#)
[取消](#)

#### # 配置接入策略。

选择“用户”页签，单击导航树中的[用户/接入策略管理/接入策略管理]菜单项，单击“增加”按钮，创建一条接入策略。

- 接入策略名输入“802.1x”。
- 证书认证选择“EAP 证书认证”。
- 证书认证类型选择“EAP-PEAP 认证”。
- 认证证书子类型选择“MS-CHAPV2 认证”。
- 下发 VLAN 输入授权下发的 VLAN “300”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 配置接入策略

用户 > 接入策略管理 > 接入策略管理 > 修改接入策略

帮助

基本信息

接入策略名 \*

802.1x

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☐ 不启用 ☒ EAP证书认证 ☐ WAP证书认证

认证证书类型

EAP-PEAP认证

认证证书子类型

MS-CHAPV2认证

下发VLAN

300

下发用户组

☐ 下发User Profile

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户MAC地址

☐ 绑定IMSI号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 禁用Windows可溶解客户端

自动重连间隔(分钟) 30

自动重连次数 3

☐ 网络故障时自动重连

违规处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务器

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式

☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定

取消

# 增加接入服务配置。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，单击“增加”按钮，创建一条接入服务。

- 服务名输入“802.1x”。
- 缺省接入策略选择之前创建的策略“802.1x”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。



图4 配置接入服务

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 \*

802.1x

服务后缀

业务分组 \*

未分组

缺省接入策略 \*

802.1x

缺省安全策略 \*

不使用

缺省内网外联配置 \*

不使用

缺省私有属性下发策略 \*

不使用

缺省BYOD页面 \*

PC - 缺省页面 (PC

服务描述

☒可申请

☐Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 安全策略 | 私有属性下发策略 | 内网外联配置 | BYOD页面 |
|-------------|------|------|----------|--------|--------|
| 未找到符合条件的记录。 |      |      |          |        |        |

确定

取消

# 增加用户配置。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，单击“增加”按钮，增加一个接入用户。

- 单击“增加用户”。
- 用户姓名输入“lw”。
- 证件号码输入“000”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 增加用户配置

用户 > 接入用户 > 增加接入用户

接入用户

接入信息

用户姓名 \*

选择

增加用户

帐号 \*

☐接开用户

☐缺省BYOD用户

☐主机名用户

☐快速认证用户

密码 \*

☒允许用户修改密码

生效时间

最大闲置时长(分钟)

Portal无感知认证最大绑定数

登录提示信息

接入服务

服务名

☐ 802.1x

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

分配IP地址

增加用户 - Mozilla Firefox

8.125.1.1/fmc/usr/user/addUserPopUpContent.xhtml

增加用户

基本信息

用户姓名 \*

lw

证件号码 \*

000

检查是否可用

通讯地址

电话

电子邮件

用户分组 \*

未分组

确定

取消

# 增加接入用户配置。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，单击“增加”按钮，增加一个接入用户。

- 单击选择选择，在页面中选择之前创建的用户“lw”。
- 账号名输入“lw”。
- 密码与密码确认输入“123456”。
- 选择服务名“802.1x”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加接入用户配置

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

lw

选择

增加用户

帐号名 \*

lw

☐ 拨开用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

时

失效时间

时

最大闲置时长(分钟)

在线数量限制

1

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                        | 服务后缀 | 状态  | 分配IP地址 |
|--------------------------------------------|------|-----|--------|
| <input checked="" type="checkbox"/> 802.1x |      | 可申请 |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

无线SSID

VLAN ID/内层VLAN ID

设备IP地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

MAC地址

IP地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

### 3.5 验证配置

# Client（IP 地址为 141.30.0.30/24）与 Local server 可以互相 ping 通，通过抓包可以看到报文并没有经过 LWAPP 封装，因此可以判断是本地转发。

图7 对访问 Local server 的数据流量采用本地转发

|     |            |             |             |      |    |                     |                                   |
|-----|------------|-------------|-------------|------|----|---------------------|-----------------------------------|
| 445 | 16.6954191 | 141.30.0.30 | 141.30.0.20 | ICMP | 82 | Echo (ping) request | id=0x0200, seq=54528/213, ttl=128 |
| 446 | 16.6959688 | 141.30.0.20 | 141.30.0.30 | ICMP | 82 | Echo (ping) reply   | id=0x0200, seq=54528/213, ttl=128 |

```

# Frame 445: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
# Ethernet II, Src: D-Link_30:69:41 (00:24:01:30:69:41), Dst: c8:be:19:e6:2b:27 (c8:be:19:e6:2b:27)
# 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 300
# Internet Protocol Version 4, Src: 141.30.0.30 (141.30.0.30), Dst: 141.30.0.20 (141.30.0.20)
# Internet Control Message Protocol

```

# Client (IP 地址为 141.30.0.30/24) 与 Enterprise internal server 可以互相 ping 通，通过抓包可以发现 Client 和 Enterprise internal server 之间的 ICMP 报文经过 LWAPP 封装通过集中式转发方式进行通信。

图8 对访问 Enterprise internalserver 的数据流量采用集中式转发

|     |            |             |             |      |     |                     |                                   |
|-----|------------|-------------|-------------|------|-----|---------------------|-----------------------------------|
| 371 | 10.6210341 | 141.30.0.30 | 8.1.1.217   | ICMP | 146 | Echo (ping) request | id=0x0200, seq=54016/211, ttl=128 |
| 372 | 10.6212291 | 8.1.1.217   | 141.30.0.30 | ICMP | 146 | Echo (ping) reply   | id=0x0200, seq=54016/211, ttl=126 |

```

# Frame 371: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
# Ethernet II, Src: 00:ef:12:34:56:00 (00:ef:12:34:56:00), Dst: Hangzhou_12:ff:01 (00:0f:e2:12:ff:01)
# Internet Protocol Version 4, Src: 141.100.0.4 (141.100.0.4), Dst: 141.100.0.1 (141.100.0.1)
# User Datagram Protocol, Src Port: 12222 (12222), Dst Port: 12222 (12222)
# LWAPP Encapsulated Packet
# IEEE 802.11 QoS Data, Flags: .....T
# Logical-Link Control
# Internet Protocol Version 4, Src: 141.30.0.30 (141.30.0.30), Dst: 8.1.1.217 (8.1.1.217)
# Internet Control Message Protocol

```

## 3.6 配置文件

- AC

```

#
port-security enable
#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
network 141.100.1.0 mask 255.255.255.0
gateway-list 141.100.1.1
#
dhcp server ip-pool vlan300
network 141.30.0.0 mask 255.255.255.0
gateway-list 141.30.0.1
#
radius scheme officel
server-type extended
primary authentication 8.1.1.5

```

```

primary accounting 8.1.1.5
key authentication cipher $c$3$EnNB6wxpjYSAJMiU2aaeNArZaBzSA13G5A==
key accounting cipher $c$3$EnNB6wxpjYSAJMiU2aaeNArZaBzSA13G5A==
user-name-format without-domain
#
domain officel
authentication lan-access radius-scheme officel
authorization lan-access radius-scheme officel
accounting lan-access none
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan forwarding-policy policy1
classifier acl 3000 behavior local
#
wlan service-template 1 crypto
ssid service1
bind WLAN-ESS 1
cipher-suite tkip
cipher-suite ccmp
security-ie rsn
service-template enable
#
wlan service-template 2 clear
ssid service2
bind WLAN-ESS 2
client forwarding-mode policy-based policy1
service-template enable
#
user-profile user
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk pvid vlan 100
port trunk permit vlan 100 300
#
interface Vlan-interface100
ip address 141.100.1.1 255.255.255.0
#
interface Vlan-interface300
ip address 141.30.0.1 255.255.255.0
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1

```

```

port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
port-security port-mode userlogin-secure-ext
port-security tx-key-type llkey
undo dot1x handshake
dot1x mandatory-domain office1
undo dot1x multicast-trigger
#
wlan ap officeap model WA2620E-AGN id 1
map-configuration apcfg.txt
serial-id 21023529G007C000020
radio 1
radio 2
    service-template 1 vlan-id 300
    service-template 2 vlan-id 300
radio enable
#
ip route-static 8.0.0.0 255.0.0.0 141.100.1.254
#
dhcp enable
#
user-profile user enable
#

```

## - Switch

```

#
vlan 10
#
vlan 100
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 10
#
interface GigabitEthernet1/0/4
port link-type access
port access vlan 10

```

```
#
interface GigabitEthernet1/0/5
port link-type access
port access vlan 300
#
interface Vlan-interface10
ip address 8.1.1.8 255.0.0.0
#
interface Vlan-interface100
ip address 141.100.1.254 255.255.255.0
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 无线接入用户延时计费典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                          |    |
|--------------------------|----|
| 1 简介.....                | 1  |
| 2 配置前提 .....             | 1  |
| 3 配置举例 .....             | 1  |
| 3.1 组网需求 .....           | 1  |
| 3.2 配置注意事项.....          | 1  |
| 3.3 配置步骤.....            | 2  |
| 3.3.1 AC 的配置 .....       | 2  |
| 3.3.2 Switch 的配置 .....   | 5  |
| 3.3.3 RADIUS 服务器的配置..... | 5  |
| 3.4 验证结果 .....           | 12 |
| 3.5 配置文件 .....           | 12 |
| 4 相关资料 .....             | 14 |



# 1 简介

本文介绍了无线控制器对无线客户端进行延时计费功能的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 和 802.1X 特性。

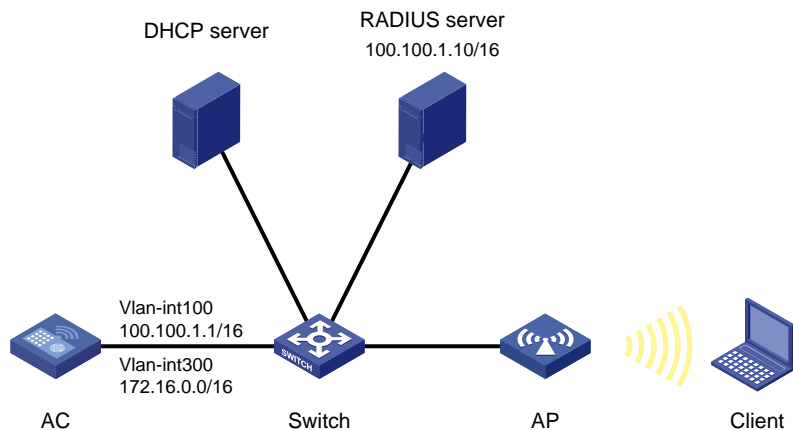
## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 通过 Switch 与 AP 相连，DHCP 服务器分别为 AP 和 Client 分配 IP 地址，RADIUS 服务器为接入的无线客户端提供认证和计费功能。为了使计费更为精确，现要求：

- 无线客户端获得 IP 地址后才向 RADIUS 服务器发送计费请求报文。
- 当无线客户端在指定的计费延时时间内没有获得分配的 IP 地址，则不发送计费请求报文，无线客户端将下线。

图1 延时计费功能组网图



### 3.2 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 在接口 WLAN-ESS 上开启 802.1X 的计费延时功能前，需要关闭服务模板，开启计费延时功能后再重新开启服务模板。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 100.100.1.1 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 100.30.1.1 255.255.0.0
[AC-Vlan-interface300] quit
```

# 配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置认证策略

# 创建 RADIUS 方案 office 并进入其视图。

```
[AC] radius scheme office
```

# 将 RADIUS 方案 office 的 RADIUS 服务器类型设置为 extended。

```
[AC-radius-office] server-type extended
```

# 设置主认证 RADIUS 服务器的 IP 地址 100.100.1.10。

```
[AC-radius-office] primary authentication 100.100.1.10
```

# 设置主计费 RADIUS 服务器的 IP 地址 100.100.1.10。

```
[AC-radius-office] primary accounting 100.100.1.10
```

# 设置系统与认证 RADIUS 服务器交互报文时的共享密钥为 admin。

```
[AC-radius-office] key authentication admin
```

# 设置系统与计费 RADIUS 服务器交互报文时的共享密钥为 admin。

```
[AC-radius-office] key accounting admin
```

# 设置设备发送 RADIUS 报文使用的源 IP 地址。

```
[AC-radius-office] nas-ip 100.100.1.1
```

# 配置发送给 RADIUS 方案 office 中 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC-radius-office] user-name-format without-domain
```

# 使能 accounting-on 功能，配置 accounting-on 报文重发时间间隔为 3 秒、accounting-on 报文的最大发送次数为 50 次（缺省情况下，报文重发时间间隔为 3 秒，最大发送次数为 50 次）。

```
[AC-radius-office] accounting-on enable interval 3 send 50
```

# 配置实时计费的时间间隔为 3 分钟。

```
[AC-radius-office] timer realtime-accounting 3
```

```
[AC-radius-office] quit
```

### (3) 配置认证域

# 创建 office 域并进入其视图。

```
[AC] domain office
```

# 为 Portal 用户配置认证方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] authentication portal radius-scheme office
```

# 为 Portal 用户配置授权方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] authorization portal radius-scheme office
```

# 为 Portal 用户配置计费方案为 RADIUS 方案，方案名为 office。

```
[AC-isp-office] accounting portal radius-scheme office
```

```
[AC-isp-office] quit
```

# 把配置的认证域 office 设置为系统缺省的 ISP 域。

```
[AC] domain default enable office
```

### (4) 配置 WLAN-ESS 接口

# 创建 WLAN-ESS 1 接口，并进入该视图。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置接口 WLAN-ESS1 的缺省 VLAN 为 VLAN 200，禁止 VLAN 1 报文通过，并允许发送 VLAN 200 报文不带 VLAN tag。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

### (5) 配置无线服务模板

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置服务模板 1 的 SSID（服务模板的标识）为 office。

```
[AC-wlan-st-1] ssid office
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 使能服务模板。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

(6) 在 AC 下绑定无线服务模板

# 创建 AP 管理模板，其名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 1 射频视图。

```
[AC-wlan-ap-officeap] radio 1
```

# 将在 AC 上配置的服务模板 1 映射到射频 1，设置绑定到射频接口的 VLAN 编号为 VLAN 300。

```
[AC-wlan-ap-officeap-radio-1] service-template 1 vlan-id 300
```

# 使能 AP 的 radio 1。

```
[AC-wlan-ap-officeap-radio-1] radio enable
```

```
[AC-wlan-ap-officeap-radio-1] quit
```

```
[AC-wlan-ap-officeap] quit
```

(7) 配置 802.1X 认证服务

# 使能端口安全。

```
[AC] port-security enable
```

# 配置 802.1X 用户的认证方式为 EAP。

```
[AC] dot1x authentication-method eap
```

# 在接口 WLAN-ESS1 上配置 802.1X 用户的强制认证域 office。

```
[AC-WLAN-ESS1] dot1x mandatory-domain office
```

# 配置端口安全模式为 userlogin-secure-ext，并使能端口 11key 类型的密钥协商功能。

```
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
```

```
[AC-WLAN-ESS1] port-security tx-key-type 11key
```

# 关闭 802.1X 的组播触发功能，以节省无线的通信带宽。

```
[AC-WLAN-ESS1] undo dot1x multicast-trigger
```

# 关闭在线用户握手功能，以避免不支持在线握手功能的客户端被强制下线。

```
[AC-WLAN-ESS1] undo dot1x handshake
```

```
[AC-WLAN-ESS1] quit
```

(8) 配置延时计费

# 关闭服务模板 1。

```
[AC] wlan service-template 1 clear
```

```
[AC-wlan-st-1] service-template disable
```

```
[AC-wlan-st-1] quit
```

# 在接口 WLAN-ESS1 上开启 802.1X 的计费延时功能，并配置计费延时时间为 5 秒，如果延时后还没有获取到 IP 地址，采取的动作作为 logoff。

```
[AC] interface wlan-ess 1
```

```
[AC-WLAN-ESS1] dot1x accounting-delay action logoff time 5
```

```
[AC-WLAN-ESS1] quit
```

# 开启服务模板 1。

```
[AC] wlan service-template 1 clear
```

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

### 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 和 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk, 禁止 VLAN 1 报文通过, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 RADIUS 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/4 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

### 3.3.3 RADIUS 服务器的配置



说明

下面以 iMC 为例 (使用 iMC 版本为: iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)) , 说明 RADIUS 服务器的基本配置。

---

# 增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置认证及计费的端口号分别为“1812”和“1813”；
- 设置与 AC 交互报文时使用的认证、计费共享密钥和确认共享密钥为“admin”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 100.100.1.1 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

帮助

接入配置

认证端口 \*1812

计费端口 \*1813

组网方式不启用混合组网

业务类型LAN接入业务

接入设备类型H3C(General)

接入设备分组无

共享密钥 \*.....

确认共享密钥 \*.....

业务分组未分组

设备列表

选择

手工增加

增加IPv6设备

全部清除

| 设备名称 | 设备IP地址      | 设备型号 | 备注 | 删除 |
|------|-------------|------|----|----|
|      | 100.100.1.1 |      |    |    |

共有1条记录。

确定

取消

# 配置接入规则。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，单击<增加>按钮，创建一条接入规则。

- 接入规则名输入“office”。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 配置接入规则

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

帮助

基本信息

接入策略名 \*

office

业务分组 \*

未分组

描述

授权信息

接入时段

无

分配IP地址 \*

否

下行速率(Kbps)

上行速率(Kbps)

优先级

☐ 启用RSA认证

证书认证

☒ 不启用 ☐ EAP证书认证 ☐ WAPI证书认证

认证证书类型

EAP-TLS认证

下发VLAN

☐ 下发User Profile

下发用户组

☐ 下发ACL

认证绑定信息

☐ 绑定接入设备IP

☐ 绑定接入设备端口

☐ 绑定VLAN

☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址

☐ 绑定用户IPv6地址

☐ 绑定用户MAC地址

☐ 绑定IMS号码

☐ 绑定计算机名称

☐ 计算机绑定域

☐ 用户必须登录到域

☐ 绑定无线SSID

☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制

☐ 启用终端硬盘序列号控制

☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端

☐ 禁用Windows可溶解客户端

☐ 禁用Linux/MacOS可溶解客户端

☐ 禁止在线修改IP地址

☐ 网络故障时自动重连

自动重连间隔(分钟) 30

自动重连次数 3

违规处理模式 ☒ 下线 ☐ 监控

☐ 禁止开设代理服务

☐ 禁止IE设置代理

☐ 禁用多网卡

☐ 禁用多操作系统

☐ 禁止认证网卡配置多IP地址

☐ 禁止修改MAC地址

☐ 禁止出现相同的MAC地址

☐ 禁用VMWare NAT服务

☐ 禁用VMWare USB服务

☐ 禁止在虚拟机中运行

IP地址获取方式

☒ 不限制 ☐ 必须静态设置 ☐ 必须动态获取

确定

取消

# 增加计费策略。

选择“用户”页签，单击导航树中的[计费业务管理/计费策略管理]菜单项，进入计费策略管理页面，在该页面中单击<增加>按钮，进入计费策略配置页面。

- 输入策略名称为“User”；
- 选择计费策略模板为“包月类型计费”；
- 设置包月基本信息：计费方式为“按时长”、计费周期为“月”、周期内固定费用为“120 元”；
- 设置包月使用量限制：允许每月最大上网使用量为 120 个小时。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 增加计费策略

用户 > 计费业务管理 > 计费策略管理 > 增加计费策略 帮助

计费策略配置

基本信息

策略名称 \*

User

计费策略模板

包月类型计费

业务分组

未分组

策略描述

包月基本信息

计费方式

按时长

周期内固定费用(元) \*

120

?

计费周期类型

月

包月使用量限制设置

周期内限制量

120

?

周期内限制单位

小时

注意

如果频繁（间隔小于30秒）修改计费策略，请进行手工生效处理。

确定

取消

# 增加服务配置。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入服务器配置管理页面，在该页面中单击<增加>按钮，进入增加服务配置页面。

- 输入服务名为“office”、服务后缀为“office”；
- 缺省接入规则输入“office”；
- 选择计费策略为“User”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。



图5 增加服务配置

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

基本信息

服务名 \*

office

服务后缀

office

业务分组 \*

未分组

缺省接入策略 \*

office

缺省私有属性下发策略 \*

不使用

计费策略 \*

User

计费周期开始类型 \*

自适应

计费周期开始日期 \*

不限

☐ 自适应连续扣费

☒ 首次计费周期按全周期计费

☐ 首次计费周期按天计费

☐ 首次计费周期免周期费

缺省BYOD页面 \*

PC - 缺省页面 (PC)

服务描述

☒ 可申请

☐ Portal无感知认证

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

# 增加用户配置。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，单击<增加>按钮，增加一个接入用户，再选择<增加用户>。

- 用户姓名输入“test”；
- 证件号码输入“1234”；
- 用户分组选择“未分组”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6 增加用户配置

增加用户

基本信息

用户姓名 \*

test

证件号码 \*

1234

检查是否可用

通讯地址

电话

电子邮件

用户分组 \*

未分组

确定

取消

# 增加接入用户配置。

返回主页面，输入：

- 账号名输入“office”；
- 密码与密码确认输入“admin”；

- 选择服务名 “office” ；
- 选择该用户所关联的接入服务为 “office”，预付金额为 “120”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图7 增加接入用户

用户 > 接入用户 > 增加接入用户

帮助

接入用户

接入信息

用户姓名 \*

test

选择

增加用户

帐号名 \*

office

☐ 预开户用户

☐ 缺省BYOD用户

☐ 主机名用户

☐ 快速认证用户

密码 \*

\*\*\*\*\*

密码确认 \*

\*\*\*\*\*

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

生效时间

失效时间

最大闲置时长(分钟)

在线数量限制

1

帐号类型

预付费

预付金额(元) \*

120

自助充值

允许

Portal无感知认证最大绑定数

1

登录提示信息

接入服务

| 服务名                                        | 服务后缀   | 状态  | 计费策略 | 分配IP地址 |
|--------------------------------------------|--------|-----|------|--------|
| <input checked="" type="checkbox"/> office | office | 可申请 | User |        |
| <input type="checkbox"/> Portal-auth       |        | 可申请 | 不计费  |        |
| <input type="checkbox"/> staff             |        | 可申请 | 不计费  |        |

接入设备绑定信息

设备序列号

端口号

外层VLAN ID

VLAN ID/内层VLAN ID

无线SSID

设备IP地址

设备IPv6地址

终端绑定信息

计算机名称

IMSI号码

Windows 域

IP地址

MAC地址

IPv6地址

提示

注意：在文本框中输入多条信息时，每行只能输入一条信息。

确定

确定并打印

取消

## 3.4 验证结果

# 在 AC 上打开 **debug** 开关。

```
<AC> debugging radius packet
```

```
<AC> terminal debugging
```

# 可以观察到 **Client** 上线，加入到无线网络中。

```
%Dec 5 10:33:47:194 2013 AC WMAC/6/WMAC_CLIENT_JOIN_WLAN: Client 001e-583f-0895
successfully joins WLAN service, on APID 1 with BSSID 0023-8930-1121.
```

..... (略)

# 观察到 **Client** 认证上线成功，通过 **802.1X** 认证，时间为 **10:33:48:769**。

```
%Dec 5 10:33:48:769 2013 AC PORTSEC/6/PORTSEC_DOT1X_LOGIN_SUCC:
-IfName=WLAN-DBSS1:13-MACAddr=00:1E:58:3F:08:95-VlanId=300-UserName=office; The user
passed 802.1X authentication and got online successfully.
```

..... (略)

# 观察到 4 秒后，AC 发送给 **RADIUS** 服务器的报文中未携带 **Client** 的 IP 地址。

```
*Dec 5 10:33:52:486 2013 AC RDS/7/DEBUG: Send attribute list:
```

```
*Dec 5 10:33:52:746 2013 AC RDS/7/DEBUG:
```

```
[32 NAS-Identifier          ] [4 ] [AC]
[5  NAS-Port                ] [6 ] [16781512]
[87 NAS_Port_Id             ] [36] [slot=1;subslot=0;port=1;vlanid=300]
[61 NAS-Port-Type           ] [6 ] [19]
[H3C-26 Connect_ID          ] [6 ] [130]
[6  Service-Type            ] [6 ] [2]
```

```
*Dec 5 10:33:53:137 2013 AC RDS/7/DEBUG:
```

```
[H3C-59 NAS-Startup-Timestamp ] [6 ] [1354557697]
```

..... (略)

# 当 **DHCP** 服务器对 **Client** 的 IP 地址池分配完毕后，**Client** 无法获取到 IP 地址，5 秒后，AC 强制 **Client** 下线，下线时间点为 **10:33:54:188**。

```
%Dec 5 10:33:54:188 2013 AC PORTSEC/6/PORTSEC_DOT1X_LOGOFF:
-IfName=WLAN-DBSS1:13-MACAddr=00:1E:58:3F:08:95-VlanId=300-UserName=office-ErrCode=1;
Session of the 802.1X user was terminated.
```

```
%Dec 5 10:33:54:208 2013 AC WMAC/6/WMAC_CLIENT_GOES_OFFLINE: Client 001e-583f-0895
disconnected from WLAN service. Reason code is 1.
```

## 3.5 配置文件

- AC:

```
#
domain default enable office
#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
```

```

server-type extended
primary authentication 100.100.1.10
primary accounting 100.100.1.10
key authentication cipher $c$3$LAeobkoqSbPOxIzI4RZav+igpYNsn4M=
key accounting cipher $c$3$LAeobkoqSbPOxIzI4RZav+igpYNsn4M=
timer realtime-accounting 3
user-name-format without-domain
nas-ip 100.100.1.1
accounting-on enable
#
domain office
authentication portal radius-scheme office
authorization portal radius-scheme office
accounting portal radius-scheme office
access-limit disable
state active
idle-cut disable
self-service-url disable
#
wlan service-template 1 clear
ssid office
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface100
ip address 100.100.1.1 255.255.0.0
#
interface Vlan-interface300
ip address 172.16.1.1 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid pvid vlan 200
port hybrid vlan 200 untagged
mac-vlan enable
port-security port-mode userlogin-secure-ext
port-security tx-key-type 11key
undo dot1x handshake
dot1x mandatory-domain cams
undo dot1x multicast-trigger
dot1x accounting-delay logoff time 5
#

```

```
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
service-template 1 vlan-id 300
radio enable
```

```
#
```

- **Switch:**

```
#
```

```
vlan 100
```

```
#
```

```
vlan 300
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port link-type trunk
```

```
port trunk permit vlan 100 300
```

```
port trunk pvid vlan 100
```

```
#
```

```
interface GigabitEthernet1/0/2
```

```
port link-type access
```

```
port access vlan 100
```

```
poe enable
```

```
#
```

```
interface GigabitEthernet1/0/3
```

```
port link-type access
```

```
port access vlan 100
```

```
#
```

```
interface GigabitEthernet1/0/4
```

```
port link-type access
```

```
port access vlan 100
```

```
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 智能带宽保障和基于 AP 的无线终端限速策略 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                               |    |
|-------------------------------|----|
| 1 简介.....                     | 1  |
| 2 配置前提 .....                  | 1  |
| 3 无线控制器智能带宽保障配置举例 .....       | 1  |
| 3.1 组网需求 .....                | 1  |
| 3.2 配置思路 .....                | 1  |
| 3.3 配置注意事项.....               | 2  |
| 3.4 配置步骤 .....                | 2  |
| 3.4.1 AC 的配置 .....            | 2  |
| 3.4.2 Switch 的配置 .....        | 4  |
| 3.5 验证配置 .....                | 5  |
| 3.6 配置文件 .....                | 5  |
| 4 基于 AP 的无线终端限速策略典型配置举例 ..... | 8  |
| 4.1 组网需求 .....                | 8  |
| 4.2 配置思路 .....                | 8  |
| 4.3 配置注意事项.....               | 8  |
| 4.4 配置步骤 .....                | 8  |
| 4.4.1 AC 的配置 .....            | 8  |
| 4.4.2 Switch 的配置 .....        | 10 |
| 4.5 验证配置 .....                | 10 |
| 4.6 配置文件 .....                | 11 |
| 5 相关资料 .....                  | 12 |



# 1 简介

本文档介绍无线控制器智能带宽保障和基于 AP 的无线终端限速策略典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WLAN 的智能带宽保障和限速的相关功能。

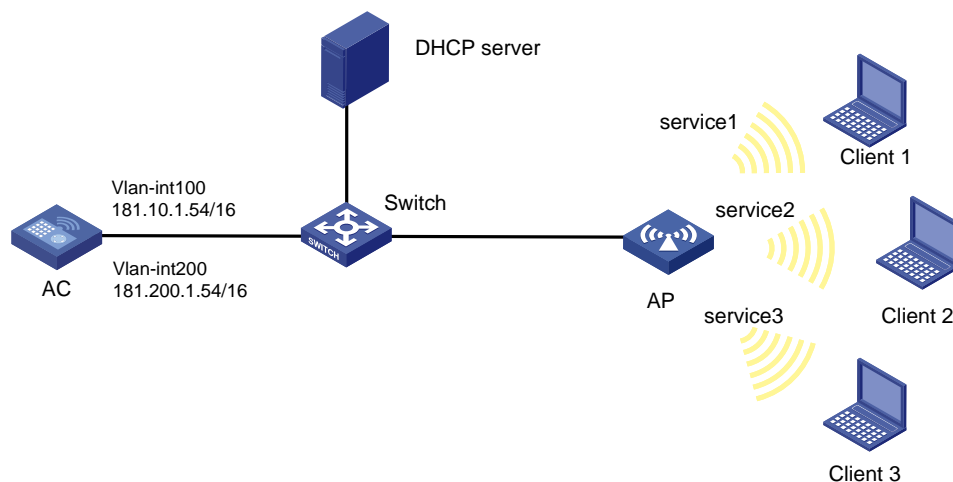
## 3 无线控制器智能带宽保障配置举例

### 3.1 组网需求

如图 1 所示，DHCP 服务器为 AP 和 Client 分配 IP 地址，Client 通过无线网络访问 Internet，具体要求如下：

- service1 接入的客户端 Client 1 能获得网络总带宽的 60%；
- service2 接入的客户端 Client 2 能获得网络总带宽的 30%；
- service3 接入的客户端 Client3 不配置带宽保障。

图1 智能带宽保障及基于 AP 的用户限速策略典型配置举例组网图



### 3.2 配置思路

为保障各客户端获取的网络带宽，使能带宽保障功能，并设置射频参考值。

### 3.3 配置注意事项

- 保障带宽的绝对值是根据射频带宽参考值及无线服务带宽占总带宽的百分比相乘计算得出的，故设置的射频带宽参考值应接近并略小于实际可达的流量上限。
- 在同一射频上绑定的所有无线服务的保障带宽百分比之和不能超过 100%。
- 智能带宽保障仅对 AP 到客户端的方向生效，即只对下行流量生效。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.4 配置步骤

#### 3.4.1 AC 的配置

##### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 181.10.1.54 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN 和 Client 接入的业务 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 进入 Vlan-interface200 的接口视图，配置 IP 地址为 181.200.1.54/16。

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 181.200.1.54 255.255.0.0
[AC-Vlan-interface200] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，禁止 VLAN1 通过，并允许 VLAN 100 和 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

##### (2) 配置无线服务

# 创建编号为 1 的 WLAN-ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口 WLAN-ESS1（Hybrid 类型）的缺省 VLAN 设置为 VLAN 200，禁止 VLAN 1 的报文通过并允许 VLAN 200 报文不带 tag 通过。

```
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```

[AC-WLAN-ESS1] port hybrid vlan 200 untagged
# 使能端口 WLAN-ESS1 的 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
# 创建一个新的服务模板（明文模板）1，设置服务模板 1 的 SSID 为 service1。
[AC] wlan service-template 1 clear
[AC-wlan-st-1] ssid service1
# 将 WLAN-ESS 接口与该服务模板绑定。
[AC-wlan-st-1] bind wlan-ess 1
# 开启服务模板 1。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
# 创建编号为 2 的 WLAN-ESS 接口。
[AC] interface wlan-ess 2
# 配置端口 WLAN-ESS2（Hybrid 类型）的缺省 VLAN 设置为 VLAN 200，禁止 VLAN 1 的报文通过并允许 VLAN 200 报文不带 tag 通过。
[AC-WLAN-ESS2] port link-type hybrid
[AC-WLAN-ESS2] port hybrid pvid vlan 200
[AC-WLAN-ESS2] undo port hybrid vlan 1
[AC-WLAN-ESS2] port hybrid vlan 200 untagged
# 使能端口 WLAN-ESS2 的 MAC VLAN 功能。
[AC-WLAN-ESS2] mac-vlan enable
[AC-WLAN-ESS2] quit
# 创建一个新的服务模板（明文模板）2，设置服务模板 2 的 SSID 为 service2。
[AC] wlan service-template 2 clear
[AC-wlan-st-2] ssid service2
# 将 WLAN-ESS 接口与该服务模板绑定。
[AC-wlan-st-2] bind wlan-ess 2
# 开启服务模板 2。
[AC-wlan-st-2] service-template enable
[AC-wlan-st-2] quit
# 创建编号为 3 的 WLAN-ESS 接口。
[AC] interface wlan-ess 3
# 配置端口 WLAN-ESS3（Hybrid 类型）的缺省 VLAN 设置为 VLAN 200，禁止 VLAN 1 的报文通过并允许 VLAN 200 报文不带 tag 通过。
[AC-WLAN-ESS3] port link-type hybrid
[AC-WLAN-ESS3] port hybrid pvid vlan 200
[AC-WLAN-ESS3] undo port hybrid vlan 1
[AC-WLAN-ESS3] port hybrid vlan 200 untagged
# 使能端口 WLAN-ESS3 的 MAC VLAN 功能。
[AC-WLAN-ESS3] mac-vlan enable
[AC-WLAN-ESS3] quit
# 创建一个新的服务模板（明文模板）3，设置服务模板 3 的 SSID 为 service3。
[AC] wlan service-template 3 clear
[AC-wlan-st-3] ssid service3

```

# 将 WLAN-ESS 接口与该服务模板绑定。

```
[AC-wlan-st-3] bind wlan-ess 3
```

# 开启服务模板 3。

```
[AC-wlan-st-3] service-template enable
```

```
[AC-wlan-st-3] quit
```

### (3) 配置 AP

# 创建一个 AP 模板，其名称为 officeap1，型号名称为 WA2620E-AGN。

```
[AC] wlan ap officeap1 model WA2620E-AGN
```

```
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
```

# 进入 radio 射频视图，将服务模板绑定到射频接口，并设置服务模板 1 和服务模板 2 的带宽保障百分比，服务模板 3 无带宽保障。

```
[AC-wlan-ap-officeap1] radio 2
```

```
[AC-wlan-ap-officeap1-radio-2] service-template 1
```

```
[AC-wlan-ap-officeap1-radio-2] service-template 2
```

```
[AC-wlan-ap-officeap1-radio-2] service-template 3
```

```
[AC-wlan-ap-officeap1-radio-2] bandwidth-guarantee enable
```

```
[AC-wlan-ap-officeap1-radio-2] bandwidth-guarantee service-template 1 percent 60
```

```
[AC-wlan-ap-officeap1-radio-2] bandwidth-guarantee service-template 2 percent 30
```

```
[AC-wlan-ap-officeap1-radio-2] radio enable
```

```
[AC-wlan-ap-officeap1-radio-2] quit
```

```
[AC-wlan-ap-officeap1] quit
```

### (4) 配置智能带宽参数

```
[AC] wlan rrm
```

```
[AC-wlan-rrm] dot11n max-bandwidth 10000
```

```
[AC-wlan-rrm] dot11a max-bandwidth 30000
```

```
[AC-wlan-rrm] dot11b max-bandwidth 7000
```

```
[AC-wlan-rrm] dot11g max-bandwidth 30000
```

```
[AC-wlan-rrm] quit
```

## 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 200，禁止 VLAN 1 通过，允许 VLAN 100 和 VLAN200 通过。

```
[Switch] interface gigabitethernet1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 200
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

## 3.5 验证配置

# 通过 **display wlan bandwidth-guarantee** 命令查看当前射频绑定的无线服务及每个无线服务配置的保障带宽。

```
<AC> display wlan bandwidth-guarantee
```

```
Bandwidth Guarantee

ST: service template

AP                               Radio   Mode                ST    Percent
Officeap1                       1      802.11n(5GHz)       1     0%
Officeap1                       1      802.11n(5GHz)       2     0%
Officeap1                       1      802.11n(5GHz)       3     0%
Officeap1                       2      802.11n(2.4GHz)     1     60%
Officeap1                       2      802.11n(2.4GHz)     2     30%
Officeap1                       2      802.11n(2.4GHz)     3     0%
```

# Client 1、Client 2 和 Client 3 分别关联到 service1、service2 和 service3，使用测试仪器 Veriwave 测试，分别向 Client 1 和 Client 2 发送大于 6000kbps 和大于 3000kbps 的下行流量，并发送给明显大于 1000kbps 的流量给 Client 3（比如 3000kbps），通过测试软件 WaveDynamix 得出下图统计数据，Client 1 和 Client 2 接收到实际的流量分别为 6000kbps 和 3000kbps 左右，Client 3 接收到的流量会受到限制，实际接收到流量约为 1000kbps 左右。

|                        | client1 - ethernet_001 to client1_001 | client2 - ethernet_001 to client2_001 | client3 - ethernet_001 to client3_001 |
|------------------------|---------------------------------------|---------------------------------------|---------------------------------------|
| Offered Load (Mbps)    | 7.2022                                | 4.1998                                | 2.9941                                |
| Forwarding Rate (Mbps) | 5.9993                                | 2.9518                                | 0.9598                                |

# 使用测试仪器 Veriwave 测试，分别向 Client 1 发送小于 6000kbps 的流量（比如 5000kbps），向 Client 2 发送小于 3000kbps 的流量（比如 2000kbps），向 Client 3 发送流量为 3000kbps 左右，通过测试软件 WaveDynamix 得出下图统计数据，Client 1 和 Client 2 实际的流量就是各自的实际流量，Client 3 接收到流量约为 3000kbps 左右。

|                        | client1 - ethernet_001 to client1_001 | client2 - ethernet_001 to client2_001 | client3 - ethernet_001 to client3_001 |
|------------------------|---------------------------------------|---------------------------------------|---------------------------------------|
| Offered Load (Mbps)    | 5.0382                                | 2.0398                                | 2.9991                                |
| Forwarding Rate (Mbps) | 5.0351                                | 2.0396                                | 2.9958                                |

## 3.6 配置文件

- AC

```
#
vlan 100
```

```

#
vlan 200
#
wlan rrm
  dot11a mandatory-rate 6 12 18 24
  dot11a supported-rate 9 36 48 54
  dot11b mandatory-rate 1 2
  dot11b supported-rate 5.5 11
  dot11g mandatory-rate 1 2 5.5 11
  dot11g supported-rate 6 9 12 18 24 36 48 54
  dot11n max-bandwidth 10000
  dot11a max-bandwidth 30000
  dot11b max-bandwidth 7000
  dot11g max-bandwidth 30000
#
wlan service-template 1 clear
  ssid service1
  bind WLAN-ESS 1
  service-template enable
#
wlan service-template 2 clear
  ssid service2
  bind WLAN-ESS 2
  service-template enable
#
wlan service-template 3 clear
  ssid service3
  bind WLAN-ESS 3
  service-template enable
#
interface Vlan-interface100
  ip address 181.10.1.54 255.255.0.0
#
interface Vlan-interface200
  ip address 181.200.1.54 255.255.0.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk pvid vlan 100
  port trunk permit vlan 100 200
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
#
interface WLAN-ESS2

```

```

port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
interface WLAN-ESS3
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap1 model WA2620E-AGN
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1
service-template 2
service-template 3
bandwidth-guarantee enable
bandwidth-guarantee service-template 1 percent 60
bandwidth-guarantee service-template 2 percent 30
radio enable
#

```

## - Switch

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
port trunk pvid vlan 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#

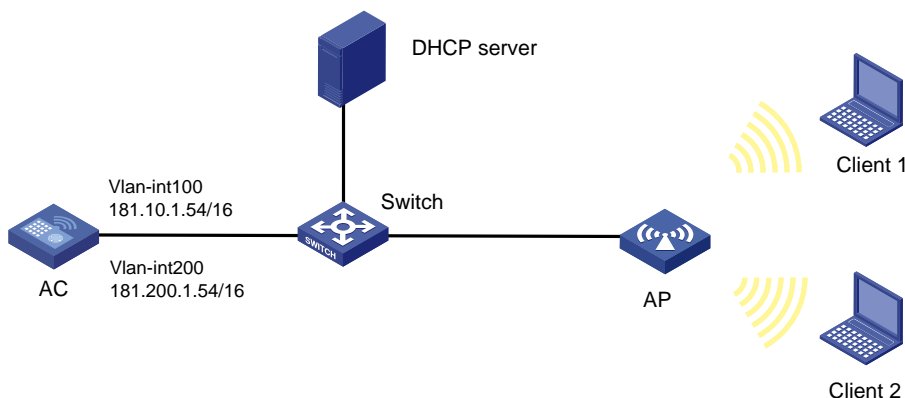
```

## 4 基于 AP 的无线终端限速策略典型配置举例

### 4.1 组网需求

如图 2 所示，DHCP 服务器为 AP 和 Client 分配 IP 地址，Client 通过无线网络访问 Internet，现要求：网络对通过 AP 射频接入的客户端做限速处理。

图2 基于 AP 的无线终端限速策略配置组网图



### 4.2 配置思路

为实现基于 AP 的无线终端限速策略，创建基于射频的限速模式，配置限速参数。

### 4.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 4.4 配置步骤

#### 4.4.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 作为 AP 与 AC 关联的 VLAN，VLAN 200 作为 WLAN-ESS 接口配置使用的 VLAN。

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 181.10.1.54 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200，VLAN 200 作为 WLAN-ESS 接口配置使用的 VLAN。



```

[AC] vlan 200
[AC-vlan200] quit
# 进入 Vlan-interface200 的接口，配置 IP 地址为 181.200.1.54/16。
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 181.200.1.54 255.255.0.0
[AC-Vlan-interface200] quit
# 配置 AC 与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型为 Trunk 类型，当前 Trunk 口的 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 和 Client 使用的 VLAN 200 通过。
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
(2) 配置无线服务
# 创建编号为 1 的 WLAN-ESS 接口。
[AC] interface wlan-ess 1
# 配置端口 WLAN-ESS1（Hybrid 类型）的缺省 VLAN 设置为 VLAN 200，禁止 VLAN 1 的报文通过并允许 VLAN 200 报文不带 tag 通过。
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
# 使能端口 WLAN-ESS1 的 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
# 创建一个新的服务模板（明文模板）1，设置服务模板 1 的 SSID 为 service1。
[AC] wlan service-template 1 clear
[AC-wlan-st-1] ssid service1
# 将 WLAN-ESS 接口与该服务模板绑定。
[AC-wlan-st-1] bind wlan-ess 1
# 开启服务模板 1。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(3) 配置 AP 并设置限速策略
# 创建一个 AP 模板，其名称为 officeap2，型号名称为 WA2620E-AGN。
[AC] wlan ap officeap2 model WA2620E-AGN
[AC-wlan-ap-officeap2] serial-id 21023529G007C000020
# 进入 radio 射频视图，将服务模板绑定到射频接口，配置静态限制 Radio 接口入方向的流量为 2000Kbps。
[AC-wlan-ap-officeap2] radio 2
[AC-wlan-ap-officeap2-radio-2] service-template 1
[AC-wlan-ap-officeap2-radio-2] client-rate-limit direction inbound mode static cir 2000
[AC-wlan-ap-officeap2-radio-2] radio enable
[AC-wlan-ap-officeap2-radio 2] quit

```

```
[AC-wlan-ap-officeap2] quit
```

#### 4.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200,其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量,VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk, 配置 PVID 为 200, 禁止 VLAN 1 的报文通过并允许 VLAN 100 和 VLAN200 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 200
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

#### 4.5 验证配置

(1) 配置 Client 1 在 officeap2 的 radio 2 上线, Client 1 的速率限制在 2000kbps 左右。

# 使用测试仪器 Veriwave 测试,通过测试软件 WaveDynamix 得出下图统计数据,发送端 OfferLoad 约为 12000Kbps, 实际 ForwardLoad 约为 2000Kbps 左右。

| client1 - client1_001 to ethernet_001 |         |
|---------------------------------------|---------|
| Offered Load (Mbps)                   | 11.9989 |
| Forwarding Rate (Mbps)                | 1.9856  |

(2) 配置 Client 1 和 Client 2 都在 officeap2 的 radio 2 上线, 如果配置的是静态固定速率为 2000kbps, 则 Client 1 和 Client 2 的速率都被限制在 2000kbps 左右。

# 使用测试仪器 Veriwave 测试,通过测试软件 WaveDynamix 得出下图统计数据, Client 1 和 Client 2 两个发送端 OfferLoad 约为 12000Kbps, 实际两者的 ForwardLoad 均约为 2000Kbps 左右。

|                        | client1 - client1_001 to ethernet_001 | client2 - client2_001 to ethernet_001 |
|------------------------|---------------------------------------|---------------------------------------|
| Offered Load (Mbps)    | 12.0001                               | 12.0063                               |
| Forwarding Rate (Mbps) | 1.9829                                | 1.9811                                |

## 4.6 配置文件

- AC

```
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
  ssid service1
  bind WLAN-ESS 1
  service-template enable
#
interface Vlan-interface100
  ip address 181.10.1.54 255.255.0.0
#
interface Vlan-interface200
  ip address 181.200.1.54 255.255.0.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk pvid vlan 100
  port trunk permit vlan 100 200
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
#
wlan ap officeap2 model WA2620E-AGN
  serial-id 21023529G007C000020
  radio 1
  radio 2
    service-template 1
    client-rate-limit direction inbound mode static cir 2000
  radio enable
#
ip route-static 0.0.0.0 255.255.0.0 181.10.1.254
#
```

- Switch

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
#
```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 逐包功率控制典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                                  |   |
|----------------------------------|---|
| 1 简介.....                        | 1 |
| 2 配置前提 .....                     | 1 |
| 3 基于丢包率的逐包功率控制配置举例 .....         | 1 |
| 3.1 组网需求 .....                   | 1 |
| 3.2 配置注意事项.....                  | 1 |
| 3.3 配置步骤 .....                   | 1 |
| 3.3.1 AC 的配置 .....               | 1 |
| 3.3.2 Switch 的配置 .....           | 3 |
| 3.4 验证配置 .....                   | 3 |
| 3.5 配置文件 .....                   | 4 |
| 4 基于 Client 信号强度的逐包功率控制配置举例..... | 5 |
| 4.1 组网需求 .....                   | 5 |
| 4.2 配置注意事项.....                  | 5 |
| 4.3 配置步骤 .....                   | 5 |
| 4.3.1 AC 的配置 .....               | 5 |
| 4.3.2 Switch 的配置 .....           | 7 |
| 4.4 验证配置 .....                   | 7 |
| 4.5 配置文件 .....                   | 7 |
| 5 相关资料 .....                     | 9 |

# 1 简介

本文档介绍了逐包功率控制典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

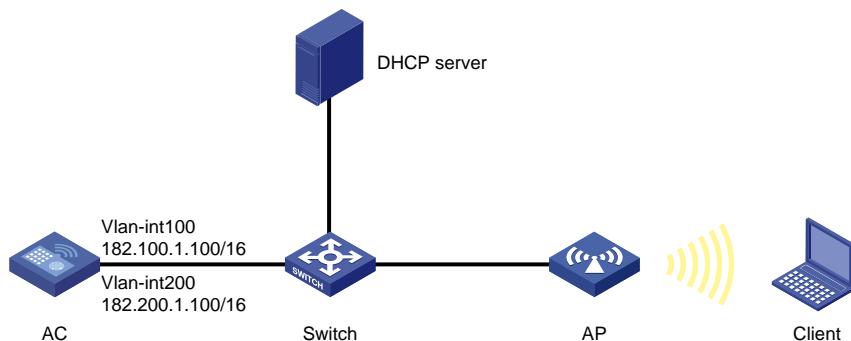
本文档假设您已了解了 WLAN 接入和 WLAN 网络应用策略中的逐包功率控制特性。

## 3 基于丢包率的逐包功率控制配置举例

### 3.1 组网需求

如[图 1](#)所示，AP 和 Client 通过 DHCP 服务器获取 IP 地址。现要求通过配置 AC 的基于丢包率的逐包功率控制功能，动态调整发射功率的大小，实现对信号覆盖范围的调整。

图1 逐包功率控制组网图



### 3.2 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 基于丢包率的逐包功率控制功能和基于 Client 信号强度的逐包功率控制功能不能同时开启。

### 3.3 配置步骤

#### 3.3.1 AC 的配置

- (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 182.100.1.100 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 配置 VLAN 200 的接口 IP 地址为 182.200.1.100/16。

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 182.200.1.100 16
[AC-Vlan-interface200] quit
```

# 创建 WLAN-ESS 1 接口，并配置 WLAN-ESS 1 接口的链路类型为 Hybrid。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

# 配置 AC 的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

## (3) 配置射频接口并绑定服务模板

# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```



```
# 设置 officeap 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-officeap-radio-2] service-template 1
# 使能 officeap 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
(4) 配置并使能基于丢包率的逐包功率控制
[AC] wlan option tpc enable
```

### 3.3.2 Switch 的配置

```
# 创建 VLAN 100 和 VLAN 200, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN
300 为无线客户端接入的 VLAN。
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk, PVID 为 100, 允许 VLAN 100
和 VLAN 200 通过。
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 100 通过, 并
使能 PoE 功能。
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口属性为 Access, 并允许 VLAN 100
通过。
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

## 3.4 验证配置

# 通过专业的测试仪器可以看到 AP 在开启逐包功率控制前后的功率发生了明显变化。

## 3.5 配置文件

- AC 的配置文件:

```
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
interface Vlan-interface100
    ip address 182.100.1.100 255.255.0.0
#
interface Vlan-interface200
    ip address 182.200.1.100 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
    serial-id 21023529G007C000020
    radio 1
    radio 2
        service-template 1
        radio enable
#
wlan option tpc enable
#
```

- Switch 的配置文件:

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
    port link-type trunk
```

```

port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
#

```

## 4 基于 Client 信号强度的逐包功率控制配置举例

### 4.1 组网需求

如 [3.1 图 1](#) 所示，AP 和 Client 通过 DHCP 服务器获取 IP 地址。现要求通过配置 AC 基于 Client 信号强度的逐包功率控制功能，实现对 AP 发送报文的发射功率的动态调整，达到对信号覆盖范围动态调整的目的。

### 4.2 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 基于丢包率的逐包功率控制功能和基于 Client 信号强度的逐包功率控制功能不能同时开启。

### 4.3 配置步骤

#### 4.3.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```

<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 182.100.1.100 16
[AC-Vlan-interface100] quit

```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN。

```

[AC] vlan 200
[AC-vlan200] quit

```

# 配置 VLAN 200 的接口 IP 地址为 182.200.1.100/16。

```

[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 182.200.1.100 16

```

```
[AC-Vlan-interface200] quit
# 创建 WLAN-ESS 1 接口，并配置 WLAN-ESS 1 接口的链路类型为 Hybrid。
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
# 使能 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
# 配置 AC 的 GigabitEthernet1/0/1 接口的链路类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 200 通过。
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

(2) 配置无线服务

```
# 创建 clear 类型的服务模板 1。
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS 1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 启用无线服务。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

(3) 配置射频接口并绑定服务模板

```
# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。
[AC] wlan ap officeap model WA2620E-AGN
# 设置 officeap 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 radio 2 射频视图。
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-officeap-radio-2] service-template 1
# 使能 officeap 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

(4) 配置并使能基于 Client 信号强度的逐包功率控制

```
# 配置当 AP 收到客户端当前数据报文的 RSSI 为 65 时，启用基于客户端信号强度的逐包功率控制功能，RSSI 调整的步长为 10，AP 发射功率下降的步长 5，AP 的最小发射功率为 10。
```

```
[AC] wlan option tpc minpower 10 powerstep 5 rssidstep 10 rssidthreshold 65 enable
```

### 4.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk, PVID 为 100, 允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN 100 通过, 并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口属性为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

## 4.4 验证配置

# 通过专业的测试仪器可以看到 AP 在开启逐包功率控制前后的功率发生了明显变化。

## 4.5 配置文件

- AC 的配置文件:

```
#
vlan 100
#
vlan 200
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
```

```

service-template enable
#
interface Vlan-interface100
ip address 182.100.1.100 255.255.0.0
#
interface Vlan-interface200
ip address 182.200.1.100 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1
radio enable
#
wlan option tpc minpower 10 powerstep 5 rssidstep 10 rssidthreshold 65 enable
#

```

- **Switch 的配置文件:**

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100

```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# 组播优化功能典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 2 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 4 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 5 |
| 4 相关资料 .....           | 6 |

# 1 简介

本文档介绍无线控制器组播优化功能典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

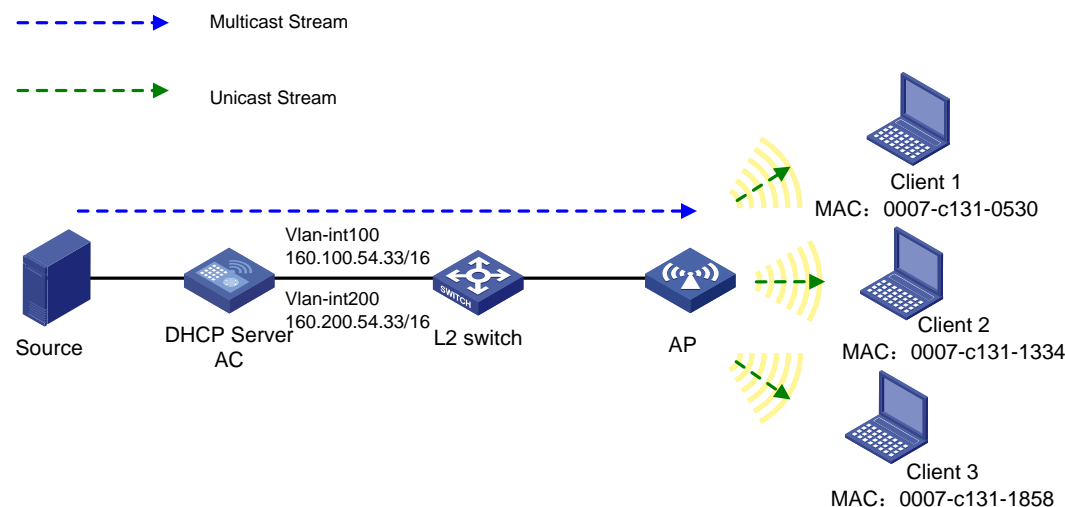
本文档假设您已了解 WLAN 组播优化特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，Client 通过接入无线网络播放组播视频，AC 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址，现要求：在 AC 上开启组播优化功能，将组播数据报文转换为单播数据报文发送给客户端，以提高组播的报文速率及减少因冲突导致的丢包。

图1 组播优化组网图



### 3.2 配置思路

AP 通过监听客户端上报的组播报告报文和离开报文进行组播优化表项维护。为了防止组播优化表项老化，配置一个组播查询器，使客户端不断的响应组播查询。

### 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.4 配置步骤

#### 3.4.1 AC 的配置

##### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 160.100.54.33 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN 和 Client 接入的业务 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
# 进入 Vlan-interface200 的接口视图，配置 IP 地址为 160.200.54.33/16。
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 160.200.54.33 16
[AC-Vlan-interface200] quit
```

# 配置 AC 与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型为 Trunk 类型，当前 Trunk 口的 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 和 Client 使用的 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

##### (2) 配置 DHCP 服务

# 开启 DHCP 服务。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 v100 为 AP 动态分配的网段为 160.100.0.0/16，网关地址为 160.100.54.32/16。

```
[AC] dhcp server ip-pool v100
[AC-dhcp-pool-v100] network 160.100.0.0 16
[AC-dhcp-pool-v100] gateway-list 160.100.54.32
[AC-dhcp-pool-v100] quit
```

# 配置 DHCP 地址池 v200 为 Client 动态分配的网段为 160.200.0.0/16，网关为 160.200.54.32/16。

```
[AC] dhcp server ip-pool v200
[AC-dhcp-pool-v200] network 160.200.0.0 16
[AC-dhcp-pool-v200] gateway-list 160.200.54.32
```

```
[AC-dhcp-pool-v200] quit
```

### (3) 配置无线接入服务和 AP 模板

# 创建编号为 1 的 WLAN-ESS 接口，配置端口的链路类型为 Hybrid，并禁止 VLAN1 通过当前的 Hybrid 端口。

```
[AC] interface wlan-ess 1
```

```
[AC-WLAN-ESS1] port link-type hybrid
```

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

# 配置端口 WLAN-ESS1 的缺省 VLAN 设置为 VLAN 200，允许 VLAN200 的报文不带 tag 通过，并开启端口基于 MAC 地址划分 VLAN 的功能。

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

# 创建一个新的服务模板（明文模板）1，设置服务模板 1 的 SSID 为 service。

```
[AC] wlan service-template 1 clear
```

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS 接口与该服务模板绑定。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 开启服务模板 1。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

# 创建一个 AP 管理模板，其名称为 officeap1，型号名称为 WA2620E-AGN，并配置序列号。

```
[AC] wlan ap officeap1 model WA2620E-AGN
```

```
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
```

# 进入 AP 的 radio 射频视图，将服务模板绑定到 radio，并开启 radio。

```
[AC-wlan-ap-officeap1] radio 2
```

```
[AC-wlan-ap-officeap1-radio-2] channel 11
```

```
[AC-wlan-ap-officeap1-radio-2] service-template 1
```

```
[AC-wlan-ap-officeap1-radio-2] radio enable
```

### (4) 开启组播优化功能以及完成组播相关的配置

# 打开组播优化功能。

```
[AC] wlan service-template 1
```

```
[AC-wlan-st-1] service-template disable
```

```
[AC-wlan-st-1] multicast optimization enable
```

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

# 全局开启 IGMP Snooping。

```
[AC] igmp-snooping
```

```
[AC-igmp-snooping] quit
```

# 在 VLAN 200 内使能 IGMP Snooping，并使能丢弃未知组播数据报文的功能。

```
[AC] vlan 200
```

```
[AC-vlan200] igmp-snooping enable
```

```
[AC-vlan200] igmp-snooping drop-unknown
```

# 将 IGMP Snooping 版本配置为 3，并使能 IGMP Snooping 查询器，配置 IGMP 普遍组查询报文的源 IP 地址为当前 VLAN 接口的 IP 地址

```
[AC-vlan200] igmp-snooping version 3
[AC-vlan200] igmp-snooping querier
[AC-vlan200] igmp-snooping general-query source-ip current-interface
[AC-vlan200] quit
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk, 当前 Trunk 口的 PVID 为 200, 禁止 VLAN 1 通过, 允许 VLAN 100 和 VLAN200 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 200
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 当前 Access 口允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

## 3.5 验证配置

- (1) 配置完成后, 组播源发起一个组播组: 230.0.1.1。Client 上线加入组播组。在 Client 上抓包可以看到组播数据包的目标 MAC 是 Client 的单播地址。
- (2) 通过下面的命令查看 AC 上生成的组播优化表项。

```
<AC> display wlan multicast optimization all

Multicast Optimization Information

AP Name: officeap1
Radio: 2
Total clients: 3
Action: Optimize
Multicast Address: 230.0.1.1
MAC Address:
0007-c131-0530, 0007-c131-1334, 0007-c131-1858
```

## 3.6 配置文件

- AC

```
#
igmp-snooping
#
vlan 100
#
vlan 200
igmp-snooping enable
    igmp-snooping version 3
    igmp-snooping drop-unknown
    igmp-snooping querier
    igmp-snooping general-query source-ip current-interface
#
dhcp server ip-pool v100
    network 160.100.0.0 mask 255.255.0.0
    gateway-list 160.100.54.32
#
dhcp server ip-pool v200
    network 160.200.0.0 mask 255.255.0.0
    gateway-list 160.200.54.32
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    multicast optimization enable
    service-template enable
#
interface Vlan-interface100
    ip address 160.100.54.33 255.255.0.0
#
interface Vlan-interface200
    ip address 160.200.54.33 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk pvid vlan 100
    port trunk permit vlan 100 200
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
```

```
wlan ap officeap1 model WA2620E-AGN id 1
    serial-id 21023529G007C000020
radio 2
    channel 11
    service-template 1
    radio enable
#
    dhcp enable
#
•   Switch
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
    port trunk pvid vlan 200
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 100
    poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“IP 组播配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“IP 组播命令参考”。

# AP 本地转发典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

|                          |   |
|--------------------------|---|
| 1 简介.....                | 1 |
| 2 配置前提 .....             | 1 |
| 3 配置举例 .....             | 1 |
| 3.1 组网需求 .....           | 1 |
| 3.2 配置思路 .....           | 1 |
| 3.3 配置注意事项.....          | 1 |
| 3.4 配置步骤 .....           | 2 |
| 3.4.1 AC 的配置 .....       | 2 |
| 3.4.2 Switch 的配置 .....   | 4 |
| 3.4.3 apcfg.txt 配置 ..... | 4 |
| 3.5 验证配置 .....           | 5 |
| 3.6 配置文件 .....           | 5 |
| 4 相关资料 .....             | 7 |

# 1 简介

本文介绍了 AP 本地转发的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

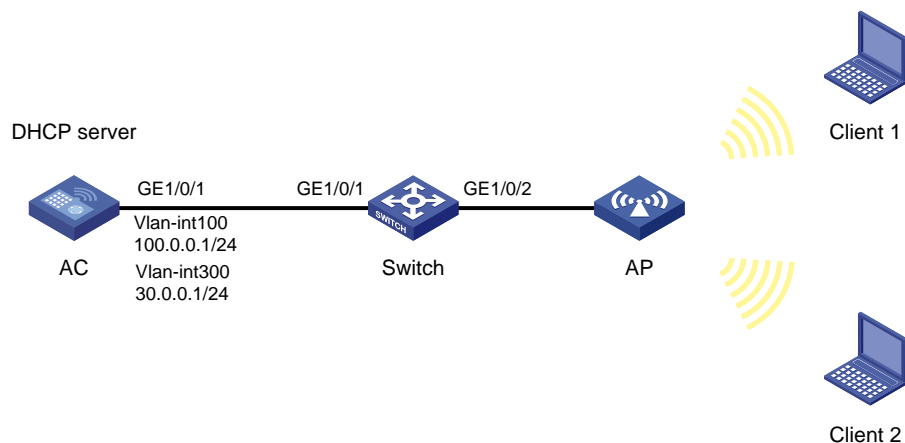
本文档假设您已了解本地转发特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 通过 Switch 连接 AP，AC 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址。现要求：在 AC 上配置 AP 本地转发功能，使 Client 的数据流量不经过 AC，直接由 AP 本地转发。

图1 AP 本地转发组网图



### 3.2 配置思路

为了使 AP 能够直接转发 Client 报文，需要在 AC 的服务模板下开启本地转发功能，同时通过下发 map-configuration 文件来对 AP 进行配置实现本地转发。

### 3.3 配置注意事项

- 在编辑 map-configuration 文件时需注意，文件的某个命令行后面不要有 Tab 键或者大量空格出线，否则会出现该行配置配不成功的情况。

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应,AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 VLAN 接口

# 创建 VLAN 100 及其对应的 VLAN 接口,并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 100.0.0.1 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN,配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan200] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 30.0.0.1 24
[AC-Vlan-interface300] quit
```

#### (2) 配置 DHCP 服务

# 创建名为 vlan100 的 DHCP 地址池,动态分配的网段为 100.0.0.0/24,网关地址为 100.0.0.1。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 100.0.0.0 mask 255.255.255.0
[AC-dhcp-pool-vlan100] gateway-list 100.0.0.1
[AC-dhcp-pool-vlan100] quit
```

# 创建名为 vlan300 的 DHCP 地址池,动态分配的网段为 30.0.0.0/24,网关地址为 30.0.0.1。

```
[AC] dhcp server ip-pool vlan300
[AC-dhcp-pool-vlan300] network 30.0.0.0 mask 255.255.255.0
[AC-dhcp-pool-vlan300] gateway-list 30.0.0.1
[AC-dhcp-pool-vlan300] quit
```

# 使能 DHCP 服务。

```
[AC] dhcp enable
```

#### (3) 配置 AC 接口

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 为 Trunk 模式,禁止 VLAN 1 报文通过,允许 VLAN 100 和 VLAN 300 通过,当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
```

```
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (4) 配置 WLAN-ESS 接口

# 创建 WLAN-ESS1 接口，并进入该视图。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置 WLAN-ESS1 接口的缺省 VLAN 为 VLAN 200，禁止 VLAN 1 报文通过，并允许 VLAN 200 报文不带 VLAN tag。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
```

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

```
[AC-WLAN-ESS1] quit
```

#### (5) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置服务模板 1 的 SSID 为 office。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 配置本地转发模式，开启 VLAN 300 的本地转发功能，即由 AP 本身进行数据帧的转发。

```
[AC-wlan-st-1] client forwarding-mode local vlan 300
```

# 开启服务模板 1。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

#### (6) 配置射频接口并绑定服务模板

# 创建 AP 管理模板，其名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 设置 radio 2 的射频类型为 802.11gn。

```
[AC-wlan-ap-officeap] radio 2 type dot11gn
```

# 将在 AC 上配置的服务模板 1 映射到射频 2，设置绑定到射频接口的 VLAN 编号为 VLAN 300。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

# 使能 AP 的 radio 2。

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

#### (7) 配置 AP 配置文件

# 在 AC 上将配置文件 apcfg.txt 下发到 AP。

```
[AC-wlan-ap-officeap] map-configuration apcfg.txt
```

```
[AC-wlan-ap-officeap] quit
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 与 AC 连接的 GigabitEthernet1/0/1 接口属性 Trunk, 禁止 VLAN 1 报文通过, 当前 Trunk 口的 PVID 为 100, 允许 VLAN 100 和 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Trunk, 当前 Trunk 口允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

### 3.4.3 apcfg.txt 配置



说明

- apcfg.txt 的内容, 要求为文本文件, 按照命令行配置的顺序编写文本文件上传至 AC 即可, AC 与 AP 关联后, 通过 **map-configuration** 命令下发至 AP 生效。从而完成对 AP 的配置。
  - map-configuration 文件可以包括 ACL、QoS、User-Profile 以及以太网口相关配置等信息, 根据具体需要进行配置。
- 

# apcfg.txt 配置文件为:

```
system-view
vlan 300
interface GigabitEthernet 1/0/1
port link-type trunk
port trunk permit vlan 100 300
```

## 3.5 验证配置

# 通过抓包可以发现 ICMP 报文不需要经过 AC 与 AP 间的隧道封装，直接转发。

图2 本地转发 ICMP 报文

| No. | Time       | Source    | Destination | Protocol | Length | Info                      |
|-----|------------|-----------|-------------|----------|--------|---------------------------|
| 1   | 0.00000000 | 100.0.0.3 | 100.0.0.1   | LWAPP    | 64     | CNTL [Malformed Packet]   |
| 2   | 0.00000000 | 100.0.0.3 | 100.0.0.1   | LWAPP    | 64     | CNTL [Malformed Packet]   |
| 3   | 0.00037068 | 100.0.0.1 | 100.0.0.3   | LWAPP    | 64     | CNTL [Malformed Packet]   |
| 4   | 0.00037273 | 100.0.0.1 | 100.0.0.3   | LWAPP    | 64     | CNTL [Malformed Packet]   |
| 5   | 0.18527436 | 30.0.0.20 | 30.0.0.10   | ICMP     | 82     | Echo (ping) request id=0x |
| 6   | 0.18527436 | 30.0.0.20 | 30.0.0.10   | ICMP     | 82     | Echo (ping) request id=0x |
| 7   | 0.18795929 | 30.0.0.10 | 30.0.0.20   | ICMP     | 82     | Echo (ping) reply id=0x   |
| 8   | 0.18796134 | 30.0.0.10 | 30.0.0.20   | ICMP     | 82     | Echo (ping) reply id=0x   |
| 9   | 0.49966284 | 100.0.0.3 | 100.0.0.1   | LWAPP    | 64     | CNTL Bad Type: 0x00       |
| 10  | 0.49966489 | 100.0.0.3 | 100.0.0.1   | LWAPP    | 64     | CNTL Bad Type: 0x00       |
| 11  | 0.81061888 | 100.0.0.2 | 100.0.0.1   | LWAPP    | 64     | CNTL [Malformed Packet]   |

Filter: Expression... Clear Apply

Frame 5: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)

Ethernet II, Src: 3com\_98:69:3d (00:1c:c5:98:69:3d), Dst: D-Link\_30:69:41 (00:24:01:30:69:41)

802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 300

Internet Protocol Version 4, Src: 30.0.0.20 (30.0.0.20), Dst: 30.0.0.10 (30.0.0.10)

Internet Control Message Protocol

## 3.6 配置文件

- AC:

```
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
network 100.0.0.0 mask 255.255.255.0
gateway-list 100.0.0.1
#
dhcp server ip-pool vlan300
network 30.0.0.0 mask 255.255.255.0
gateway-list 30.0.0.1
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
client forwarding-mode local vlan 300
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
```

```

port trunk pvid vlan 100
#
interface Vlan-interface100
ip address 100.0.0.1 255.255.255.0
#
interface Vlan-interface300
ip address 30.0.0.1 255.255.255.0
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN
map-configuration apcfg.txt
serial-id 21023529G007C000020
radio 1
radio 2
service-template 1 vlan-id 300
radio enable

```

```

#
dhcp enable
#

```

## - Switch

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 100 300
port trunk pvid vlan 100
poe enable
#

```

## - apcfg.txt:

```

system-view
vlan 300
interface GigabitEthernet 1/0/1
port link-type trunk
port trunk permit vlan 100 300

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。



# IAG 业务板支持 PEAP 认证典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                           |    |
|---------------------------|----|
| 1 简介.....                 | 1  |
| 2 配置前提 .....              | 1  |
| 3 配置举例 .....              | 1  |
| 3.1 组网需求 .....            | 1  |
| 3.2 配置思路 .....            | 2  |
| 3.3 配置注意事项 .....          | 2  |
| 3.4 配置步骤 .....            | 2  |
| 3.4.1 AC 的配置 .....        | 2  |
| 3.4.2 IAG 的配置 .....       | 4  |
| 3.4.3 Switch 的配置 .....    | 6  |
| 3.4.4 RADIUS 服务器的配置 ..... | 7  |
| 3.5 验证配置 .....            | 11 |
| 3.6 配置文件 .....            | 12 |
| 4 相关资料 .....              | 15 |

# 1 简介

本文档介绍 IAG 业务板支持 PEAP 认证典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

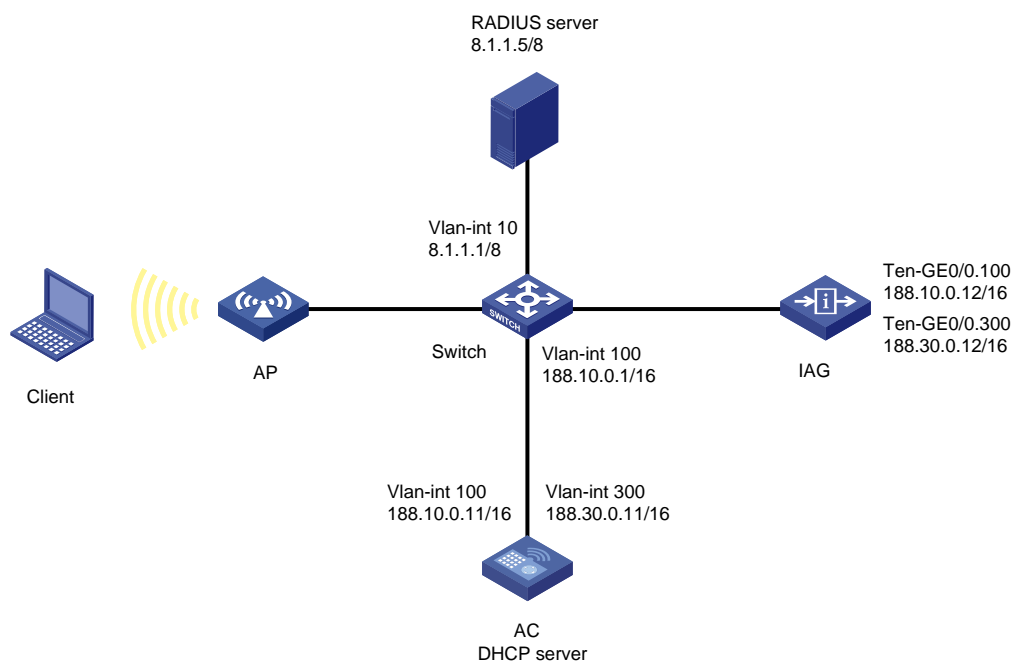
本文档假设您已了解 WLAN 无线接入、802.1X 等特性。

## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，本举例按照 AC+IAG 方式进行组网，AC 作为 DHCP 服务器为 Client 和 AP 分配 IP 地址，AC 和 AP 通过交换机相连。现要求无线用户接入无线网络时在 IAG 上做 PEAP 认证，在 AC 上进行加密。

图1 无线控制器 IAG 业务板支持 PEAP 认证组网图



## 3.2 配置思路

- IAG 上面三层口支持 802.1X 认证，但不支持加密方式的 802.1X 认证，需要在 AC 上配置加密功能，并使用代理，将认证指向 IAG。
- 配置漫游隧道来实现 AC 与 IAG 之间 Client 的同步。

## 3.3 配置注意事项

- IAG 上配置的 nas-ip 要与 RADIUS 服务器上添加设备时使用的地址一致。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 开启代理功能，代理设备与被代理设备必须处于同一漫游组中，且一台代理设备只能代理一台其他设备。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 188.10.0.11 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 及其对应的 VLAN 接口，并为该接口配置 IP 地址，该 VLAN 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 188.20.0.11 16
[AC-Vlan-interface200] quit
```

# 创建 VLAN 300 及其对应的 VLAN 接口，并为该接口配置 IP 地址，该 VLAN 作为 Client 接入的业务 VLAN。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 188.30.0.11 16
[AC-Vlan-interface300] quit
```

# 将与 Switch 相连的接口 Bridge-Aggregation 1 的链路类型配置为 Trunk，配置 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100、VLAN 200 和 VLAN 300 通过。

```
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] port link-type trunk
```

```
[AC-Bridge-Aggregation1] port trunk permit vlan 100 200 300
[AC-Bridge-Aggregation1] undo port trunk permit vlan 1
[AC-Bridge-Aggregation1] quit
```

## (2) 配置 DHCP

# 在 AC 上开启 DHCP 服务。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 vlan100 为 AP 动态分配的网段为 188.10.0.0/16，网关地址为 188.10.0.11。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 188.10.0.0 16
[AC-dhcp-pool-vlan100] gateway-list 188.10.0.11
[AC-dhcp-pool-vlan100] quit
```

# 配置 DHCP 地址池 vlan300 为 Client 动态分配的网段为 188.30.0.0/16，网关地址为 188.30.0.11。

```
[AC] dhcp server ip-pool vlan300
[AC-dhcp-pool-vlan300] network 188.30.0.0 16
[AC-dhcp-pool-vlan300] gateway-list 188.30.0.11
[AC-dhcp-pool-vlan300] quit
```

## (3) 配置 802.1X 认证

# 使能端口安全。

```
[AC] port-security enable
```

# 配置 dot1x 认证方式为 eap。

```
[AC] dot1x authentication-method eap
```

# 配置 WLAN-ESS 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
```

# WLAN-ESS 接口下配置 dot1x 认证。

```
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
```

# 使能 11key 类型的密钥协商功能

```
[AC-WLAN-ESS1] port-security tx-key-type 11key
```

# 关闭 802.1X 多播触发功能和在线用户握手功能。

```
[AC-WLAN-ESS1] undo dot1x multicast-trigger
[AC-WLAN-ESS1] undo dot1x handshake
```

# 使能远程代理认证功能。即 802.1X 用户需要在 AC 上面进行 11key 协商加解密，IAG 插卡上面负责认证和控制报文的转发。

```
[AC-WLAN-ESS1] port-security remote-auth-proxy enable
[AC-WLAN-ESS1] quit
```

# 创建服务模板 1（加密类型服务模板）。

```
[AC] wlan service-template 1 crypto
```

# 配置 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 设置信标和探查响应帧携带 RSN IE。

```
[AC-wlan-st-1] security-ie rsn
```

# 配置加密方式为 ccmp。

```
[AC-wlan-st-1] cipher-suite ccmp
```

# 开启服务模板。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

#### (4) 配置 AP

# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的加密类型的服务模板 1 与射频 2 进行关联，并设置绑定到射频接口的 VLAN 编号。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
```

# 使能 AP 的 radio2。

```
[AC-wlan-ap-officeap-radio-2] radio enable
```

```
[AC-wlan-ap-officeap-radio-2] quit
```

```
[AC-wlan-ap-officeap] quit
```

#### (5) 配置漫游组

# 配置漫游组，AC 通过 VLAN 100 与 IAG 板卡建立漫游隧道。

```
[AC] wlan mobility-group systemgroup
```

```
[AC-wlan-mg-systemgroup] source ip 188.10.0.11
```

```
[AC-wlan-mg-systemgroup] member ip 188.10.0.12
```

# 使能漫游组。

```
[AC-wlan-mg-systemgroup] mobility-group enable
```

```
[AC-wlan-mg-systemgroup] quit
```

#### (6) 配置代理功能

# 开启 SNMP 代理功能，AC 对 IAG 插卡进行代理。

```
[AC] snmp-agent proxy ip 188.10.0.12
```

# 开启 ARP Snooping 功能后可以在 AC 上显示学习到的 Client 的 IP 地址。

```
[AC] arp-snooping enable
```

### 3.4.2 IAG 的配置

#### (1) 配置 IAG 的接口

# 创建 VLAN 100、VLAN 300。其中 VLAN 100 作为漫游隧道的 VLAN，VLAN 300 作为无线用户接入 VLAN，同时 VLAN100 作为与 RADIUS Server 通信的 VLAN。

```
<IAG> system-view
```

```
[IAG] vlan 100
```

```

[IAG-vlan100] quit
[IAG] vlan 300
[IAG-vlan300] quit
# 配置子接口 Ten-GigabitEthernet 0/0.100，并配置 IP 地址为 188.10.0.12/16。
[IAG] interface ten-gigabitethernet 0/0.100
# 使能当前接口的 Dot1q 终结功能，并指定当前接口能够终结的 VLAN 报文的最外层 VLAN ID 为 100。
[IAG-Ten-GigabitEthernet0/0.100] vlan-type dot1q vid 100
[IAG-Ten-GigabitEthernet0/0.100] ip address 188.10.0.12 255.255.0.0
[IAG-Ten-GigabitEthernet0/0.100] quit
# 配置子接口 Ten-GigabitEthernet 0/0.300，并配置 IP 地址为 188.30.0.12/16。
[IAG] interface ten-gigabitethernet 0/0.300
# 使能当前接口的 Dot1q 终结功能，并指定当前接口能够终结的 VLAN 报文的最外层 VLAN ID 为 300。
[IAG-Ten-GigabitEthernet0/0.300] vlan-type dot1q vid 300
[IAG-Ten-GigabitEthernet0/0.300] ip address 188.30.0.12 255.255.0.0
[IAG-Ten-GigabitEthernet0/0.300] quit
(2) 配置 802.1X 认证
# 使能端口安全。
[IAG] port-security enable
# 配置 dot1x 认证方式为 eap。
[IAG] dot1x authentication-method eap
# 配置认证服务器。
[IAG] radius scheme office
# 配置主认证 RADIUS 服务器的 IP 地址。
[IAG-radius-office] primary authentication 8.1.1.5
# 配置与认证 RADIUS 服务器交互报文时的共享密钥。
[IAG-radius-office] key authentication 123456
# 配置发送给 RADIUS 服务器的用户名不携带域名。
[IAG-radius-office] user-name-format without-domain
# 设置发送 RADIUS 报文使用的源地址。
[IAG-radius-office] nas-ip 188.10.0.12
[IAG-radius-office] quit
# 配置认证域。
[IAG] domain office
# 配置 dot1x 用户使用 RADIUS 方案 office 进行认证、授权，不计费。
[IAG-isp-office] authentication lan-access radius-scheme office
[IAG-isp-office] authorization lan-access radius-scheme office
[IAG-isp-office] accounting lan-access none
# 子接口下配置 dot1x 认证。
[IAG] interface ten-gigabitethernet 0/0.300
[IAG-Ten-GigabitEthernet0/0.300] port-security port-mode userlogin-secure-ext
# 关闭 dot1x 多播触发功能和在线用户握手功能。
[IAG-Ten-GigabitEthernet0/0.300] undo dot1x handshake

```

```
[IAG-Ten-GigabitEthernet0/0.300] undo dot1x multicast-trigger
# 配置 dot1x 认证域为 office。
[IAG-Ten-GigabitEthernet0/0.300] dot1x mandatory-domain office
# 配置允许无线用户接入。
[IAG-Ten-GigabitEthernet0/0.300] port-security wlan-access
[IAG-Ten-GigabitEthernet0/0.300] quit
(3) 配置漫游组
# 配置漫游组，IAG 通过 VLAN 100 与 AC 建立漫游隧道。
[IAG] wlan mobility-group systemgroup
[IAG-wlan-mg-systemgroup] source ip 188.10.0.12
[IAG-wlan-mg-systemgroup] member ip 188.10.0.11
# 使能漫游组。
[IAG-wlan-mg-systemgroup] mobility-group enable
[IAG-wlan-mg-systemgroup] quit
(4) 配置到 RADIUS 服务器的路由
# 配置静态路由，其目的地址为 8.1.1.1/8，指定下一跳为 188.10.0.1。
[IAG] ip route-static 8.1.1.1 8 188.10.0.1
```

### 3.4.3 Switch 的配置

```
# 创建 VLAN 10、VLAN 100 和 VLAN 300，其中 VLAN 10 用于连接 RADIUS 服务器，VLAN 100
用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN。
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，允许
VLAN 10、100 和 VLAN 300 通过。
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 10 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 RADIUS 服务器相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 10
通过。
```



```
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 10
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 IAG 相连的 GigabitEthernet1/0/4 接口的属性为 Trunk，配置 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/4] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

# 配置 VLAN 10 的接口地址为 8.1.1.1/8，用于连接 RADIUS 服务器。

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 8.1.1.1 8
[Switch-Vlan-interface10] quit
```

# 配置 VLAN 100 的接口地址为 188.10.1.1/16

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 188.10.0.1 16
[Switch-Vlan-interface100] quit
```

### 3.4.4 RADIUS 服务器的配置



说明

下面以 iMC 作为 RADIUS 服务为例（使用 iMC 版本为：iMC PLAT 7.0(E0202)、iMC UAM 7.0(E0202)），说明 RADIUS 服务器的配置。

#### # 增加接入设备

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，单击<增加>按钮，进入“增加接入设备”页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“123456”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“LAN 接入业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 188.10.0.12 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备

| 接入配置   |              |          |         |
|--------|--------------|----------|---------|
| 认证端口 * | 1812         | 计费端口 *   | 1813    |
| 组网方式   | 不启用混合组网      | 业务类型     | LAN接入业务 |
| 接入设备类型 | H3C(General) | 接入设备分组   | 无       |
| 共享密钥 * | *****        | 确认共享密钥 * | *****   |
| 业务分组   | 未分组          |          |         |

| 设备列表    |             |      |    |    |
|---------|-------------|------|----|----|
| 选择      | 手工增加        | 全部清除 |    |    |
| 设备名称    | 设备IP地址      | 设备型号 | 备注 | 删除 |
|         | 188.10.0.12 |      |    |    |
| 共有1条记录。 |             |      |    |    |

## # 配置接入策略

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，点击<增加>按钮，进入增加接入策略页面。

- 接入策略名填写 eap-peap。
- 证书认证选择“EAP 证书认证”。
- 认证证书类型选择“EAP-PEAP 认证”。
- 认证证书子类型选择“MS-CHAPV2 认证”。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 接入策略管理 > 接入策略管理 > 修改接入策略 帮助

基本信息

接入策略名 \*

eap-peap

业务分组 \*

未分组

描述

授权信息

接入时段

无

?

下行速率(Kbps)

优先级

证书认证

☐ 不启用
☒ EAP证书认证
☐ WAP证书认证

认证证书类型

EAP-PEAP认证

下发VLAN

☐ 下发User Profile
☐ 下发ACL

分配IP地址 \*

否

上行速率(Kbps)

☐ 启用RSA认证

认证证书子类型

MS-CHAPV2认证

下发用户组

?

认证绑定信息

☐ 绑定接入设备IP
☐ 绑定接入设备端口
☐ 绑定VLAN
☐ 绑定QinQ双VLAN

☐ 绑定用户IP地址
☐ 绑定用户MAC地址
☐ 绑定IMSI号码
☐ 绑定计算机名称

☐ 计算机绑定域
☐ 用户必须登录到域
☐ 绑定无线SSID
☐ 绑定接入设备序列号

☐ 启用终端MAC地址控制
☐ 启用终端硬盘序列号控制
☐ 启用无线SSID控制

用户客户端配置

☐ 仅限iNode客户端
☐ 禁用Windows可卸载客户端
☐ 网络故障时自动重连

☐ 禁用Linux/MacOS可卸载客户端

自动重连间隔(分钟)

30

☐ 禁止在线修改IP地址

自动重连次数

3

违规处理模式

☒ 下线
☐ 监控

☐ 禁止开设代理服务器
☐ 禁止认证网卡配置多IP地址
☐ 禁用VMWare USB服务

☐ 禁止IE设置代理
☐ 禁止修改MAC地址
☐ 禁止在虚拟机中运行

☐ 禁用多网卡
☐ 禁止出现相同的MAC地址

☐ 禁用多操作系统
☐ 禁用VMWare NAT服务

IP地址获取方式

☒ 不限制
☐ 必须静态设置
☐ 必须动态获取

确定

取消

## # 配置接入服务

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，点击<增加>按钮，进入增加接入服务页面。

- 服务名填写“eap-peap”。
- 缺省接入策略选择“eap-peap”。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务 帮助

基本信息

服务名 \*

eap-peap

业务分组 \*

未分组

缺省私有属性下发策略 \*

不使用

?

缺省BYOD页面 \*

PC - 缺省页面 (PC)

服务描述

☒ 可申请

?

☐ Portal无感知认证

?

服务后缀

缺省接入策略 \*

eap-peap

?

接入场景列表

增加

| 名称          | 接入策略 | 私有属性下发策略 | BYOD页面 | 优先级 | 修改 | 删除 |
|-------------|------|----------|--------|-----|----|----|
| 未找到符合条件的记录。 |      |          |        |     |    |    |

确定

取消

## # 配置接入用户

9

选择“用户”页签，单击导航树中的[增加用户]菜单项，进入增加用户页面。

- 用户姓名填写 **test**。
- 证件号码填写 **123**。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。

用户 > 增加用户 帮助

**增加用户**

基本信息

|        |      |        |     |        |
|--------|------|--------|-----|--------|
| 用户姓名 * | test | 证件号码 * | 123 | 检查是否可用 |
| 通讯地址   |      | 电话     |     | ?      |
| 电子邮件   |      | 用户分组 * | 未分组 |        |

☐ 开通自助帐户

确定 取消

添加用户完成后，会跳转到增加用户结果页面，单击[增加用户账号]进入“增加接入用户”视图。

用户 > 增加用户结果 帮助

增加用户完成，您可继续选择如下操作：

|          |               |
|----------|---------------|
| 增加用户帐号   | 增加接入用户帐号。     |
| 返回用户列表   | 返回用户列表。       |
| 查看用户详细信息 | 查看刚刚增加的用户的信息。 |
| 继续增加用户   | 继续增加新的用户。     |

在“增加接入用户”视图下。

- 账户名填写 “**test**”。
- 密码填写 “**123456**”。
- 接入服务选择配置的接入服务 “**eap-peap**”。
- 其他配置采用页面默认配置即可。
- 单击<确定>按钮完成操作。



Online=00h00m53s

# 在 IAG 上通过命令 **display connection ucibindex** 可以看到 MAC 地址为 24-77-03-41-E2-F4 的用户在 IAG 上进行认证，认证方式为 EAP。

```
[IAG] display connection ucibindex 67
```

```
Index=67 , Username=test@office
```

```
MAC=24-77-03-41-E2-F4
```

```
IP=N/A
```

```
IPv6=N/A
```

```
Access=8021X , AuthMethod=EAP
```

```
Port Type=Wireless-802.11, Port Name=Ten-GigabitEthernet0/0.300
```

```
Initial VLAN=N/A, Authorization VLAN=N/A
```

```
ACL Group=Disable
```

```
User Profile=N/A
```

```
CAR=Disable
```

```
Priority=Disable
```

```
Start=2014-04-30 16:48:32 , Current=2014-04-30 17:21:23 , Online=00h32m50s
```

```
Total 1 connection matched.
```

## 3.6 配置文件

- AC

```
#
port-security enable
#
dot1x authentication-method eap
#
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
network 188.10.0.0 mask 255.255.0.0
gateway-list 188.10.0.11
#
dhcp server ip-pool vlan300
network 188.30.0.0 mask 255.255.0.0
gateway-list 188.30.0.11
#
wlan service-template 1 crypto
ssid service
bind WLAN-ESS 1
cipher-suite ccmp
security-ie rsn
service-template enable
#
```

```

interface Bridge-Aggregation1
  port link-type trunk
  port trunk permit vlan 100 200 300
#
interface Vlan-interface100
  ip address 188.10.0.11 255.255.0.0
#
interface Vlan-interface200
  ip address 188.20.0.11 255.255.0.0
#
interface Vlan-interface300
  ip address 188.30.0.11 255.255.0.0
#
interface WLAN-ESS1
  port link-type hybrid
  port hybrid vlan 200 untagged
  port hybrid pvid vlan 200
  mac-vlan enable
  port-security port-mode userlogin-secure-ext
  port-security tx-key-type 11key
  port-security remote-auth-proxy enable
  undo dot1x handshake
  undo dot1x multicast-trigger
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
  radio 2
    channel 6
    service-template 1 vlan-id 300
  radio enable
#
wlan mobility-group systemgroup
  member ip 188.10.0.12
  source ip 188.10.0.11
  mobility-group enable
#
snmp-agent proxy ip 188.10.0.12
#
dhcp enable
#
arp-snooping enable
#
•   IAG
#
port-security enable
#
dot1x authentication-method eap

```

```

#
vlan 100
#
vlan 200
#
vlan 300
#
radius scheme office
    primary authentication 8.1.1.5
    key authentication 123456
    user-name-format without-domain
    nas-ip 188.10.0.12
#
domain office
    authentication lan-access radius-scheme office
    authorization lan-access radius-scheme office
    accounting lan-access none
    access-limit disable
    state active
    idle-cut disable
    self-service-url disable
domain system
    access-limit disable
    state active
    idle-cut disable
    self-service-url disable
#
interface Ten-GigabitEthernet0/0.100
    vlan-type dot1q vid 100
    ip address 188.10.0.12 255.255.0.0
#
interface Ten-GigabitEthernet0/0.300
    vlan-type dot1q vid 300
    ip address 188.30.0.12 255.255.0.0
    port-security port-mode userlogin-secure-ext
    port-security wlan-access
    undo dot1x handshake
    dot1x mandatory-domain office
    undo dot1x multicast-trigger
#
wlan mobility-group systemgroup
    member ip 188.10.0.11
    source ip 188.10.0.12
    mobility-group enable
#
ip route-static 8.0.0.0 8 188.10.0.1
#

```

- Switch



```

#
vlan 10
#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10 100 300
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 poe enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 100 300
 port trunk pvid vlan 100
#
interface Vlan-interface10
 ip address 8.1.1.1 255.0.0.0
#
interface Vlan-interface100
 ip address 188.10.0.1 255.255.0.0
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。

# RSN 安全服务 ESS 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 1 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 3 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 5 |
| 4 相关资料 .....           | 6 |

## 1 简介

本文档介绍 RSN 安全服务 ESS 配置案例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

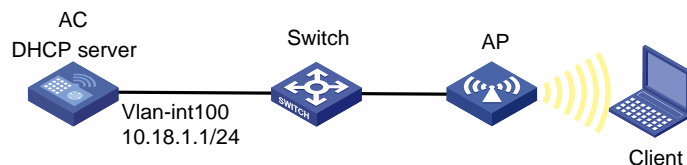
本文档假设您已了解 WLAN 安全特性。

### 3 配置举例

### 3.1 组网需求

如图 1 所示，AP 通过交换机与 AC 相连，AC 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址，通过配置 AP 提供 SSID 为 office-rsn 的加密方式无线接入，确保用户可以安全可靠的传输数据。

图1 RSN 安全服务 ESS 配置举例组网图



### 3.2 配置思路

为实现 AP 提供 RSN 加密方式的无线接入，配置无线服务功能，使用 **open-system** 方式认证并在 WLAN 服务模板视图下使能安全信息元素。

### 3.3 配置注意事项

- 开启无线侧的端口安全功能时，请确保该端口的 **802.1X** 功能或 **MAC** 地址认证功能处于关闭状态。
- 对于无线局域网来说，**802.1X** 认证可以由客户端主动发起认证，或由无线模块发现用户后自动触发认证，而不需要通过端口定期发送 **802.1X** 的组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 **802.1X** 组播触发功能。
- 配置 **AP** 的序列号时请确保该序列号与 **AP** 唯一对应，**AP** 的序列号可以通过 **AP** 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 启动端口安全

# 在 AC 上开启端口安全功能。

```
<AC> system-view
[AC] port-security enable
```

#### (2) 配置 AC 的 IP 地址

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。同时 VLAN 100 作为无线用户接入的 VLAN。

```
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-int-vlan-100] ip address 10.18.1.1 24
[AC-int-vlan-100] quit
```

#### (3) 配置 DHCP 服务

# 使能 DHCP 服务。

[AC] dhcp enable

# 配置 DHCP 地址池 vlan100 为 AP 和 Client 动态分配的网段为 10.18.1.0/24, 网关地址为 10.18.1.1。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 10.18.1.0 24
[AC-dhcp-pool-vlan100] gateway-list 10.18.1.1
[AC-dhcp-pool-vlan100] quit
```

#### (4) 配置 AC 的接口

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，当前 Trunk 口的 PVID 为 100, 禁止 VLAN1 通过, 允许 VLAN 100 (AC 和 AP 间建立 LWAPP 隧道和无线用户接入的 VLAN) 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (5) 配置无线服务

# 创建编号为 1 的 WLAN-ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 100，禁止 VLAN1 通过并允许 VLAN100 不带 tag 通过。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 100
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 100 untagged
```

# 在 WLAN-ESS1 端口上使能 MAC VLAN 功能。

```

[AC-WLAN-ESS1] mac-vlan enable
# 配置 WLAN-ESS1 的端口安全模式为 psk。
[AC-WLAN-ESS1] port-security port-mode psk
# 在接口 WLAN-ESS1 下使能 11key 类型的密钥协商功能。
[AC-WLAN-ESS1] port-security tx-key-type 11key
# 在接口 WLAN-ESS1 下配置预共享密钥为 12345678。
[AC-WLAN-ESS1] port-security preshared-key pass-phrase 12345678
# 关闭 802.1X 的组播触发功能。
[AC-WLAN-ESS1] undo dot1x multicast-trigger
[AC-WLAN-ESS1] quit
# 创建 crypto 类型的服务模板 1。
[AC] wlan service-template 1 crypto
# 设置当前服务模板的 SSID 为 office-rsn。
[AC-wlan-st-1] ssid office-rsn
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 设置无线客户端接入该无线服务（SSID）的认证方式为开放式系统认证。
[AC-wlan-st-1] authentication-method open-system
# 启用 CCMP 加密套件。
[AC-wlan-st-1] cipher-suite ccmp
# 配置信标和探查帧携带 RSN IE 信息。
[AC-wlan-st-1] security-ie rsn
# 使能服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit

```

#### (6) 配置 AP

```

# 创建 AP 管理模板，其名称为 officeap，型号名为 WA2620E-AGN。
[AC] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 设置 radio 2 的无线接口工作在 2.4GHZ 的 802.11gn 模式。
[AC-wlan-ap-officeap] radio 2 type dot11gn
# 设置 radio 2 的工作信道为 6。
[AC-wlan-ap-officeap-radio-2] channel 6
# 将服务模板 1 绑定到 AP 的 radio 2 上。
[AC-wlan-ap-officeap-radio-2] service-template 1
# 使能 AP 的 radio 2。
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] return

```

### 3.4.2 Switch 的配置

```

# 创建 VLAN 100，用于转发 AC 和 AP 间 LWAPP 隧道内的流量和无线用户的接入。
<Switch> system-view

```

```
[Switch] vlan 100
[Switch-vlan100] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk, 当前 Trunk 口的 PVID 为 100,, 禁止 VLAN1 通过, 允许 VLAN 100 通过。
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access, 当前 Access 口允许 VLAN100 通过。
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

### 3.5 验证配置

# 使用 **display wlan client verbose** 命令, 可以看到客户端采用 RSN、CCMP 加密认证方式接入无线网络。

```
[AC] display wlan client verbose
Total Number of Clients          : 1
                                Client Information
-----
MAC Address                      : 0021-631e-7911
User Name                        : -NA-
AID                              : 1
AP Name                          : officeap
Radio Id                         : 2
SSID                             : office-rsn
BSSID                           : 5866-ba28-2b70
Port                             : WLAN-DBSS1:9
VLAN                             : 100
State                            : Running
Power Save Mode                  : Active
Wireless Mode                    : 11gn
Channel Band-width               : 20MHz
SM Power Save Enable             : Disabled
Short GI for 20MHz                : Supported
Short GI for 40MHz               : Not Supported
Support MCS Set                  : 0,1,2,3,4,5,6,7,8,9,
                                10,11,12,13,14,15,16,17,18,19,
                                20,21,22,23
BLOCK ACK-TID 0                  : BOTH
```

```

BLOCK ACK-TID 1 : OUT
BLOCK ACK-TID 7 : OUT
QoS Mode : WMM
Listen Interval (Beacon Interval) : 1
RSSI : 42
Rx/Tx Rate : 39/144.4
Client Type : WPA2(RSN)
Authentication Method : Open System
Authentication Mode : Central
AKM Method : PSK
4-Way Handshake State : PTKINITDONE
Group Key State : IDLE
Encryption Cipher : AES-CCMP
Roam Status : Normal
Roam Count : 0
Up Time (hh:mm:ss) : 00:05:10

```

## 3.6 配置文件

- AC

```

#
port-security enable
#
vlan 1
#
vlan 100
#
dhcp server ip-pool vlan100
network 10.18.1.0 mask 255.255.255.0
gateway-list 10.18.1.1
#
wlan service-template 1 crypto
ssid office-rsn
bind WLAN-ESS 1
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk pvid 100
port trunk permit vlan 100
#
interface Vlan-interface100
ip address 10.18.1.1 255.255.255.0
#
interface WLAN-ESS1

```



```

port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 100 untagged
port hybrid pvid vlan 100
mac-vlan enable
port-security port-mode psk
port-security tx-key-type 11key
port-security preshared-key pass-phrase cipher $c$3$p9xuVvRgvfEf/g4EkCs0fQ//fdJ
xLIliGAay
undo dot1x multicast-trigger
#
wlan ap officeap model WA2620E-AGN id 1
serial-id 21023529G007C000020
radio 1
radio 2
channel 6
service-template 1
radio enable
#
dhcp enable
#
• Switch
#
vlan 100
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 定时自动开启无线射频功能典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 1 |
| 3.4 配置步骤 .....         | 1 |
| 3.4.1 AC 的配置 .....     | 1 |
| 3.4.2 Switch 的配置 ..... | 4 |
| 3.5 验证配置 .....         | 5 |
| 3.6 配置文件 .....         | 8 |
| 4 相关资料 .....           | 9 |

# 1 简介

本文介绍了使用定时执行任务功能自动开启无线射频的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

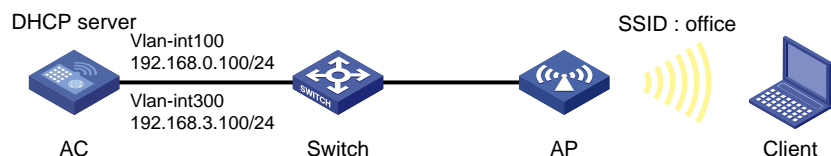
本文档假设您已了解定时执行任务功能和 WLAN 接入的特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，Client 访问无线网络，AC 通过 Switch 连接 AP，AC 充当 DHCP 服务器，为 AP 和 Client 分配 IP 地址。现要求：配置定时执行任务功能，每天 8:00 开启 AC 上所有关联 AP 的 Radio 接口，每天 20:00 关闭 AC 上所有关联 AP 的 Radio 接口。

图1 定时执行任务功能自动开启无线射频组网图



### 3.2 配置思路

为了使 Client 能够连接到无线网络，需要在 AC 上配置 WLAN 服务模板、AP 管理模板和 WLAN-ESS 接口，并将 WLAN-ESS 接口绑定到服务模板上。

### 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

### 3.4 配置步骤

#### 3.4.1 AC 的配置

- (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.0.100 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 192.168.3.100 24
[AC-Vlan-interface300] quit
```

# 配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

## (2) 配置 DHCP 服务

# 创建名为 vlan100 的 DHCP 地址池，地址池范围为 192.168.0.200~192.168.0.250，网关地址为 192.168.0.100。

```
[AC] dhcp server ip-pool vlan100 extended
[AC-dhcp-pool-vlan100] network ip range 192.168.0.200 192.168.0.250
[AC-dhcp-pool-vlan100] network mask 255.255.255.0
[AC-dhcp-pool-vlan100] gateway-list 192.168.0.100
[AC-dhcp-pool-vlan100] quit
```

# 创建名为 vlan300 的 DHCP 地址池，地址池范围为 192.168.3.200~192.168.3.250，网关地址为 192.168.3.100。

```
[AC] dhcp server ip-pool vlan300 extended
[AC-dhcp-pool-vlan300] network ip range 192.168.3.200 192.168.3.250
[AC-dhcp-pool-vlan300] network mask 255.255.255.0
[AC-dhcp-pool-vlan300] gateway-list 192.168.3.100
[AC-dhcp-pool-vlan300] quit
```

# 使能 DHCP 服务。

```
[AC] dhcp enable
```

# 在 VLAN 100 接口上应用 DHCP 地址池 vlan100。

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] dhcp server apply ip-pool vlan100
[AC-Vlan-interface100] quit
```

# 在 VLAN 300 接口上应用 DHCP 地址池 vlan300。

```
[AC] interface vlan-interface 300
[AC-Vlan-interface300] dhcp server apply ip-pool vlan300
[AC-Vlan-interface300] quit
```

### (3) 配置 WLAN-ESS 接口

# 创建 WLAN-ESS 1 接口，并进入该视图。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置接口 WLAN-ESS 1 的缺省 VLAN 为 VLAN 200，禁止 VLAN 1 报文通过，并允许 VLAN 200 报文不带 VLAN tag。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

### (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置服务模板 1 的 SSID（服务模板的标识）为 office。

```
[AC-wlan-st-1] ssid office
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 开启服务模板。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### (5) 配置射频接口并绑定服务模板

# 创建 AP 名称为 ap1，型号名称为 WA2620E-AGN，序列号为 210235A29G007C000020。

```
[AC] wlan ap ap1 model WA2620E-AGN
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

# 进入 AP 的 radio 1 射频视图。

```
[AC-wlan-ap-ap1] radio 1
```

# 将在 AC 上配置的服务模板 1 映射到射频 1，设置绑定到射频接口的 VLAN 编号为 VLAN 300。

```
[AC-wlan-ap-ap1-radio-1] service-template 1 vlan-id 300
```

# 使能 AP 的 radio 1。

```
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
```

# 进入 AP 的 radio 2 射频视图。

```
[AC-wlan-ap-ap1] radio 2
```

# 将在 AC 上配置的服务模板 1 映射到射频 2，设置绑定到射频接口的 VLAN 编号为 VLAN 300。

```
[AC-wlan-ap-ap1-radio-2] service-template 1 vlan-id 300 300
```

# 使能 AP 的 radio 2。

```
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
(6) 配置定时执行任务
# 创建定时执行任务 radio_disable，并进入定时执行任务视图。
[AC] job radio_disable
# 配置运行指定命令的视图为 system 系统视图。
[AC-job-radio_disable] view system
# 配置定时执行任务，使设备在每天 20: 00 关闭所有 radio。
[AC-job-radio_disable] time 1 repeating at 20:00 command wlan radio disable all
[AC-job-radio_disable] time 2 repeating at 20:00 command y
[AC-job-radio_disable] quit
# 创建定时执行任务 radio_enable，并进入定时执行任务视图。
[AC] job radio_enable
# 配置运行指定命令的视图为 system 系统视图。
[AC-job-radio_enable] view system
# 配置定时执行任务，使设备在每天 8: 00 开启所有 radio。
[AC-job-radio_enable] time 1 repeating at 08:00 command wlan radio enable all
[AC-job-radio_enable] time 2 repeating at 08:00 command y
[AC-job-radio_enable] quit
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 300，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线客户端接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
```

# 配置 Switch 和 AC 相连的 GigabitEthernet1/0/1 接口属性 Trunk，禁止 VLAN 1 报文通过，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 和 VLAN 300 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，当前 Access 口允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

## 3.5 验证配置

# 在AC上通过命令行 **display wlan ap name ap1 verbose** 查看 ap1 radio的管理状态 Admin State, 在 8:00~20:00, radio 的管理状态为 UP, 在其它时间 radio 的管理状态为 DOWN。

```
[AC] display wlan ap name ap1 verbose
```

```
AP Profile: ap1
```

```
-----
APID                               : 1
AP System Name                     : Not Configured
Map Configuration                   : Not Configured
State                              : Run
Up Time(hh:mm:ss)                  : 00:01:17

Model                              : WA2620E-AGN
Serial-ID                          : 210235A29G007C000020
IP Address                         : 192.168.0.200

H/W Version                        : Ver.A
S/W Version                        : V500R002B109D024SP01
Boot-Rom Version                   : 1.23
Description                        : Not Configured

Connection Type                    : Master
Peer AC MAC Address                : -NA-
Priority Level                      : 7
Echo Interval(s)                   : 10
Statistics report Interval(s)      : 50

Cir(Kbps)                         : -NA-
Cbs(Bytes)                         : -NA-

Jumboframe Threshold               : Disable

Transmitted control packets        : 34
Received control packets           : 34
Transmitted data packets           : 0
Received data packets              : 0

Configuration Failure Count        : 0
Last Failure Reason                 :

Last Reboot Reason                  : Tunnel Initiated

Latest IP Address                   : 192.168.0.200
Tunnel Down Reason                  : No Reason
Connection Count                   : 1
-----
```

```
AP Mode                            : Split
```



```

AP operation mode           : Normal
Portal Service             : Enable
Device Detection           : Disable
Maximum Number of Radios   : 2
Current Number of Radios   : 2
Client Keep-alive Interval : Disable
Client Idle Interval(s)    : 3600
Broadcast-probe Reply Status : Enable
Radio 1:
    Basic BSSID             : 0023-893c-c1c0
    Current BSS Count       : 3
    Running Clients Count   : 0
    Wireless Mode           : 11an
    Client Dot11n-only      : Disabled
    Channel Band-width      : 20/40MHz
    Secondary Channel Offset : SCA
    HT Protection Mode      : non-member protection
    Short GI for 20MHz      : Not supported
    Short GI for 40MHz      : Supported
    Mandatory MCS Set       : 0, 1, 2, 3, 4, 5, 6, 7
    Support MCS Set         : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
    A-MSDU                  : Enabled
    A-MPDU                  : Enabled
    Configured Channel      : auto(149)
    Configured Power (dBm)  : 16 auto(14)
    Interference (%)        : -NA-
    Channel Load (%)        : -NA-
    Utilization (%)         : -NA-
    Co-channel Neighbor Count : -NA-
    Channel Health          : -NA-
    Radio Policy            : default_rp
    Service Template        : 1
    SSID                    : office
    Port                    : WLAN-DBSS1:3000
    Mesh Policy              : default_mp_plcy
    ANI Support              : Enable
    Admin State              : UP
    Physical State           : UP
    Operational Rates (Mbps):
        6                   : mandatory
        9                   : supported
        12                  : mandatory
        18                  : supported
        24                  : mandatory
        36                  : supported
        48                  : supported
        54                  : supported
    Radar detected Channels  : None

```

Radio 2:

|                           |                                                        |
|---------------------------|--------------------------------------------------------|
| Basic BSSID               | : 0023-893c-c1d0                                       |
| Current BSS Count         | : 3                                                    |
| Running Clients Count     | : 0                                                    |
| Wireless Mode             | : 11gn                                                 |
| Client Dot11n-only        | : Disabled                                             |
| Channel Band-width        | : 20MHz                                                |
| Secondary Channel Offset  | : SCN                                                  |
| HT Protection Mode        | : non-member protection                                |
| Short GI for 20MHz        | : Not supported                                        |
| Short GI for 40MHz        | : Supported                                            |
| Mandatory MCS Set         | : 0, 1, 2, 3, 4, 5, 6, 7                               |
| Support MCS Set           | : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 |
| A-MSDU                    | : Enabled                                              |
| A-MPDU                    | : Enabled                                              |
| Configured Channel        | : auto(1)                                              |
| Configured Power (dBm)    | : 19 auto(14)                                          |
| Interference (%)          | : -NA-                                                 |
| Channel Load (%)          | : -NA-                                                 |
| Utilization (%)           | : -NA-                                                 |
| Co-channel Neighbor Count | : -NA-                                                 |
| Channel Health            | : -NA-                                                 |
| Preamble Type             | : short                                                |
| Radio Policy              | : 2                                                    |
| Service Template          | : 1                                                    |
| SSID                      | : office                                               |
| Port                      | : WLAN-DBSS1:3003                                      |
| Mesh Policy               | : default_mp_plcy                                      |
| ANI Support               | : Enable                                               |
| 11g Protection            | : Disable                                              |
| Admin State               | : UP                                                   |
| Physical State            | : UP                                                   |
| Operational Rates (Mbps): |                                                        |
| 1                         | : mandatory                                            |
| 2                         | : mandatory                                            |
| 5.5                       | : mandatory                                            |
| 6                         | : supported                                            |
| 9                         | : supported                                            |
| 11                        | : mandatory                                            |
| 12                        | : supported                                            |
| 18                        | : supported                                            |
| 24                        | : supported                                            |
| 36                        | : supported                                            |
| 48                        | : supported                                            |
| 54                        | : supported                                            |
| Radar detected Channels   | : None                                                 |

## 3.6 配置文件

- AC:

```
#
job radio_disable
    view system
    time 1 repeating at 20:00 command wlan radio disable all
    time 2 repeating at 20:00 command y
job radio_enable
    view system
    time 1 repeating at 08:00 command wlan radio enable all
    time 2 repeating at 08:00 command y
#
dhcp server ip-pool vlan100 extended
    network ip range 192.168.0.200 192.168.0.250
    network mask 255.255.255.0
    gateway-list 192.168.0.100
#
dhcp server ip-pool vlan300 extended
    network ip range 192.168.3.200 192.168.3.250
    network mask 255.255.255.0
    gateway-list 192.168.3.100
#
vlan 100
#
vlan 200
#
vlan 300
#
wlan service-template 1 clear
    ssid office
    bind WLAN-ESS 1
    service-template enable
#
interface Vlan-interface100
    ip address 192.168.0.100 255.255.255.0
    dhcp server apply ip-pool vlan100
#
interface Vlan-interface300
    ip address 192.168.3.100 255.255.255.0
    dhcp server apply ip-pool vlan300
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 300
    undo port trunk permit vlan 1
    port trunk pvid vlan 100
#
```

```

interface WLAN-ESS1
  port link-type hybrid
  port hybrid pvid vlan 200
  undo port hybrid vlan 1
  port hybrid vlan 200 untagged
  mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
  serial-id 210235A29G007C000020
  radio 1
    service-template 1 vlan-id 300
    radio enable
  radio 2
    service-template 1 vlan-id 300
    radio enable
#
dhcp enable
#

```

#### • Switch:

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100
  undo port trunk permit vlan 1
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 100
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“基础配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“基础命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# AP 管理组典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置注意事项 .....       | 2 |
| 3.4 配置步骤 .....         | 2 |
| 3.4.1 AC 的配置 .....     | 2 |
| 3.4.2 Switch 的配置 ..... | 3 |
| 3.5 验证配置 .....         | 4 |
| 3.6 配置文件 .....         | 5 |
| 4 相关资料 .....           | 6 |

# 1 简介

本文介绍了通过 AP 组管理功能开启 AP 组内成员 AP 的射频并绑定到指定服务模板功能的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

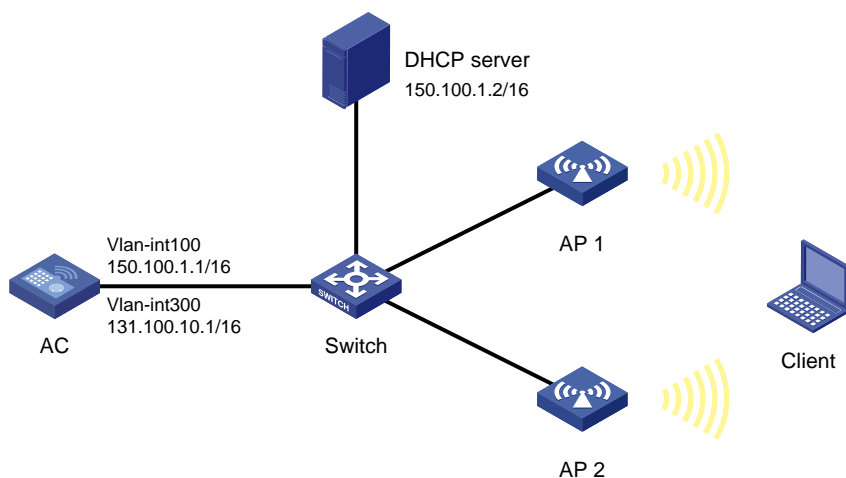
本文档假设您已了解 WLAN 的 AP 组管理相关功能。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，AC 通过 Switch 与 AP 相连，DHCP 服务器分别为 Client 和 AP 分配 IP 地址，各个 AP 所需的配置相同。为简化 AC 的配置，减少重复配置工作，现要求：在 AC 上配置 AP 组功能，将 AP 组配置映射到 AP 组内成员 AP，使 AP 组内的成员 AP 完成自动批量配置。

图1 AP 组管理组网图



### 3.2 配置思路

为了使 Client 通过 AP 组内成员 AP 接入 WLAN 网络，需要将无线服务模板绑定到 AP 组。

## 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

#### (1) 配置 AC 接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 150.100.1.1 16
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 WLAN-ESS 接口的缺省 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 创建 VLAN 300 作为 Client 接入的业务 VLAN，配置 VLAN 300 的接口 IP 地址。

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface300
[AC-Vlan-interface300] ip address 131.100.10.1 16
[AC-Vlan-interface300] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 300 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过，允许 VLAN 200 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```



## (2) 配置无线服务

# 创建 **clear** 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 **SSID** 为 **service**。

```
[AC-wlan-st-1] ssid service
```

# 将 **WLAN-ESS1** 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

## (3) 创建 AP 组

# 创建 **AP 1** 的管理模板，名称为 **officeap1**，型号选择 **WA2620E-AGN**，并配置序列号。

```
[AC] wlan ap officeap1 model WA2620E-AGN
```

```
[AC-wlan-ap-officeap1] serial-id 210235A29G007C000020
```

```
[AC-wlan-ap-officeap1] quit
```

# 创建 **AP 2** 的管理模板，名称为 **officeap2**，型号选择 **WA2620E-AGN**，并配置序列号。

```
[AC] wlan ap officeap2 model WA2620E-AGN
```

```
[AC-wlan-ap-officeap2] serial-id 210235A29G007C000021
```

```
[AC-wlan-ap-officeap2] quit
```

# 创建 **AP 组** 名称为 **test-group**，将 **officeap1** 和 **officeap2** 加入 **AP 组** 内。

```
[AC] wlan ap-group test-group
```

```
[AC-ap-group-test-group] ap officeap1
```

```
[AC-ap-group-test-group] ap officeap2
```

## (4) 配置 AP 组的无线接入功能

# 将服务模板 1 映射到 **AP 组** 内成员 **AP** 的 **2.4GHz** 射频，设置绑定到射频接口的 **VLAN** 编号为 **VLAN 300**。

```
[AC-ap-group-test-group] dot11bg service-template 1 vlan-id 300
```

# 开启 **AP 组** 内成员 **AP** 的 **2.4GHz** 射频。

```
[AC-ap-group-test-group] dot11bg radio enable
```

```
[AC-ap-group-test-group] quit
```

## 3.4.2 Switch 的配置

# 创建 **VLAN 100** 和 **VLAN 300**，其中 **VLAN 100** 用于转发 **AC** 和 **AP** 间 **LWAPP** 隧道内的流量，**VLAN 300** 为无线客户端接入的 **VLAN**。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 300
```

```
[Switch-vlan300] quit
```

# 配置 **Switch** 与 **AC** 相连的 **GigabitEthernet1/0/1** 接口属性 **Trunk**，禁止 **VLAN 1** 报文通过，当前 **Trunk** 口的 **PVID** 为 **100**，允许 **VLAN 100** 和 **VLAN 300** 通过。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 300
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN 100 通过。
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/4 接口属性为 Access，并允许 VLAN 100 通过。
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

### 3.5 验证配置

# 使用 **display wlan ap all** 命令查看到 AP 1、AP 2 与 AC 已经建立连接。

```
[AC] display wlan ap all
Total Number of APs configured          : 2
Total Number of configured APs connected : 2
Total Number of auto APs connected      : 0
AP Profiles
State : I = Idle,   J = Join, JA = JoinAck,   IL = ImageLoad
       C = Config, R = Run,   KU = KeyUpdate, KC = KeyCfm
       M = Master, B = Backup
-----
AP Name                               State Model                               Serial-ID
-----
officeap1                             R/M    WA2620E-AGN                               210235A29G007C000020
officeap2                             R/M    WA2620E-AGN                               210235A29G007C000021
-----
```

# 使用 **display wlan client** 命令用来查看无线客户端的信息，观察到 Client 从 SSID service 接入，能成功上线。

```
<AC> display wlan client
Total Number of Clients                  : 1
Client Information
```

|                |           |          |            |      |
|----------------|-----------|----------|------------|------|
| SSID: service  |           |          |            |      |
| -----          |           |          |            |      |
| MAC Address    | User Name | APID/RID | IP Address | VLAN |
| -----          |           |          |            |      |
| 0015-0062-6580 | -NA-      | 1 /2     | 0.0.0.0    | 300  |
| -----          |           |          |            |      |

## 3.6 配置文件

```
#
vlan 100
#
vlan 200
#
vlan 300
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
wlan ap-group test-group
    ap officeap1
    ap officeap2
    dot11bg service-template 1 vlan-id 300
    dot11bg radio enable
#
interface Vlan-interface100
    ip address 150.100.1.1 255.255.0.0
#
interface Vlan-interface300
    ip address 131.100.10.1 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 300
    undo port trunk permit vlan 1
    port trunk pvid vlan 100
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
    mac-vlan enable
#
wlan ap officeap1 model WA2620E-AGN id 1
    serial-id 210235A29G007C000020
```

```

radio 1
radio 2
  service-template 1 vlan-id 300
  radio enable
#
wlan ap officeap2 model WA2620E-AGN id 2
  serial-id 210235A29G007C000021
  radio 1
  radio 2
    service-template 1 vlan-id 300
    radio enable
#

```

- **Switch:**

```

#
vlan 100
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 300
  undo port trunk permit vlan 1
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/4
  port link-type access
  port access vlan 100
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# WIAA 构建安全无线网络典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 使用限制 .....           | 1 |
| 4 配置举例 .....           | 1 |
| 4.1 组网需求 .....         | 1 |
| 4.2 配置思路 .....         | 2 |
| 4.3 配置注意事项 .....       | 2 |
| 4.4 配置步骤 .....         | 2 |
| 4.4.1 AC 的配置 .....     | 2 |
| 4.4.2 Switch 的配置 ..... | 4 |
| 4.5 验证配置 .....         | 4 |
| 4.6 配置文件 .....         | 5 |
| 5 相关资料 .....           | 7 |

# 1 简介

本文档介绍了 WIAA 构建安全无线网络的典型配置举例。

WIAA (Wireless Intelligent Application Aware, 无线智能业务感知), 可提供基于无线端口的访问控制, 通过在无线接口上的出方向上应用防火墙的 **Packet-Filter**, 入方向上应用 **ASPF** 策略, 能够拒绝有线网络直接访问无线用户, 但不影响无线用户的访问权限, 确保了无线网络内的安全。

## 2 配置前提

本文档不严格与具体软、硬件版本对应, 如果使用过程中与产品实际情况有差异, 请参考相关产品手册, 或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证, 配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置, 为了保证配置效果, 请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解无线 WIAA 特性。

## 3 使用限制

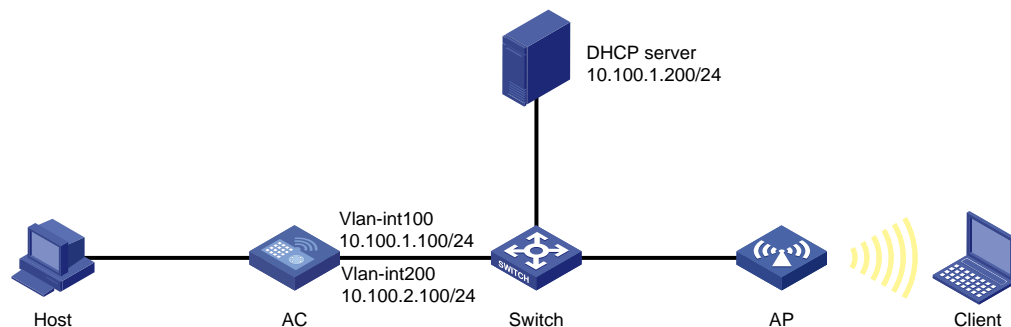
本文涉及的包过滤防火墙和 **ASPF** 功能需要用户购买 **License**, 并完成注册之后才能使用。**License** 可以通过购买特性软件授权书获得, 授权书上提供了注册 WIAA 特性需要使用的 **License** 授权码及特性功能说明。详细的操作流程, 请参见《H3C WX 系列无线控制产品 **License** 激活申请和注册操作指导》, 添加 **License** 的相关配置请参见“基础配置指导”中的“**License** 管理配置”。

## 4 配置举例

### 4.1 组网需求

如图 1 所示, AC 与 AP 通过二层交换机相连, DHCP 服务器为 AP 和 Client 分配 IP 地址, 为了保护无线网络的安全, 通过在 AC 上部署 **ASPF** 功能和 **ACL** 规则, 可以限制有线网络中的主机 Host 对无线用户 Client 的访问, 但不影响 Client 访问 Host。

图1 通过 WIAA 构建安全无线网络配置组网图



## 4.2 配置思路

- 为了阻止 Host 主动访问 Client，需要创建 ACL 规则，并应用于防火墙 Packet-Filter。
- 为了保证 Client 向 Host 发送的请求报文，以及 Host 对 Client 的应答报文可以正常通过 AC，需要在 AC 上创建防火墙 ASPF 策略。

## 4.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 在无线接口上应用防火墙策略时需要注意接口的出方向应用 Packet-Filter 策略，接口的入方向应用 ASPF 策略。
- 基于无线接口的防火墙只能对二层的流量进行有效过滤。

## 4.4 配置步骤

### 4.4.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.100.1.100 24
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 配置 VLAN 200 的接口 IP 地址为 192.168.2.100/24

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.168.2.100 255.255.255.0
[AC-Vlan-interface200] quit
```

# 配置 AC 与 Switch 相连的 GigabitEthernet1/0/2 接口的类型为 Trunk，PVID 为 100，允许 VLAN 100 和 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] port link-type trunk
[AC-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/2] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/2] quit
```

# 创建 WLAN-ESS 1 接口，并设置端口的链路类型为 Hybrid。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。



```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
```

# 在 Hybrid 端口上使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

## (2) 配置防火墙策略

# 配置 ACL 2000，并创建规则，拒绝所有流量通过。

```
[AC] acl number 2000
[AC-acl-basic-2000] rule deny
[AC-acl-basic-2000] quit
```

# 创建 ASPF 策略 1，缺省情况下，ASPF 检测处于开启状态，故采用缺省配置。

```
[AC] aspf-policy 1
[AC-aspf-policy-1] quit
```

# 在无线接口的入方向应用防火墙 ASPF 策略。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] firewall aspf 1 inbound
```

# 在无线接口的出方向应用防火墙包过滤。

```
[AC-WLAN-ESS1] firewall packet-filter 2000 outbound
[AC-WLAN-ESS1] quit
```

# 全局下使能防火墙开关。

```
[AC] firewall enable
```

## (3) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS 1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 使能无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

## (4) 配置射频接口并绑定服务模板

# 创建 AP 的管理模板，名称为 officeap，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 进入 radio 2 射频视图。

```
[AC-wlan-ap-officeap] radio 2
```

# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联。

```
[AC-wlan-ap-officeap-radio-2] service-template 1 vlan-id 200
```

# 使能 AP 的 radio 2。

```
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
```

## 4.4.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的链路类型为 Trunk, PVID 为 100, 并允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口的链路类型为 Access, 并允许 VLAN 100 通过, 并使能 PoE 功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口的链路类型为 Access, 并允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

## 4.5 验证配置

(1) 无线用户成功上线后, 可以访问有线网络中的主机。

# 从 Client ping 有线网络中 Host, 可以 ping 通。

```
D:\> ping 192.168.3.1
```

```
Pinging 192.168.3.1 with 32 bytes of data:
```

```
Reply from 192.168.3.1: bytes=32 time=19ms TTL=254
Reply from 192.168.3.1: bytes=32 time<1ms TTL=254
Reply from 192.168.3.1: bytes=32 time<1ms TTL=254
Reply from 192.168.3.1: bytes=32 time<1ms TTL=254
```

```
Ping statistics for 192.168.3.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

# 在 AC 上使用 **display session table verbose** 命令查看 session 信息:

```
[AC] display session table verbose
Initiator:
  Source IP/Port : 192.168.3.2/2048
  Dest IP/Port   : 192.168.3.1/1
  VPN-InClientnce/VLAN ID/VLL ID: 3
Responder:
  Source IP/Port : 192.168.3.1/0
  Dest IP/Port   : 192.168.3.2/1
  VPN-Instance/VLAN ID/VLL ID: 3
Pro: ICMP(1)    App: unknown      State: ICMP-CLOSED
Start time: 2013-11-19 11:07:14  TTL: 27s
Received packet(s)(Init): 4 packet(s) 240 byte(s)
Received packet(s)(Reply): 4 packet(s) 240 byte(s)
```

(2) 无线用户成功上线后, Host 不能访问 Client。

# 在 Host 上 ping Client, 不能 ping 通。

```
D:\> ping 192.168.3.2
```

```
Pinging 192.168.3.2 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 192.168.3.2:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

# 在 AC 上使用 **display firewall-statistics interface** 命令查看防火墙过滤信息, 统计数据如下:

```
[AC] display firewall-statistics interface WLAN-DBSS1:1
Interface: WLAN-DBSS1:1
Out-bound Policy: acl 2000
From 2013-11-19 11:14:24 to 2013-11-19 11:14:51
  0 packets, 0 bytes, 0% permitted,
  5 packets, 420 bytes, 100% denied,
  0 packets, 0 bytes, 0% permitted default,
  0 packets, 0 bytes, 0% denied default,
Totally 0 packets, 0 bytes, 0% permitted,
Totally 5 packets, 420 bytes, 100% denied.
```

## 4.6 配置文件

- AC 的配置文件:

```
#
firewall enable
#
acl number 2000
rule 0 deny
```

```

#
vlan 100
#
vlan 200
#
aspf-policy 1
#
wlan service-template 1 clear
    ssid service
    bind WLAN-ESS 1
    service-template enable
#
wlan ap-group default_group
    ap officeap
#
interface Vlan-interface100
    ip address 10.100.1.100 255.255.255.0
#
interface Vlan-interface200
    ip address 192.168.2.100 255.255.255.0
#
interface GigabitEthernet1/0/2
    port link-type trunk
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#
interface WLAN-ESS1
    port link-type hybrid
    undo port hybrid vlan 1
    port hybrid vlan 200 untagged
    port hybrid pvid vlan 200
mac-vlan enable
    firewall packet-filter 2000 outbound
    firewall aspf 1 inbound
#
wlan ap officeap model WA2620E-AGN id 1
    serial-id 21023529G007C000020
    radio 1
    radio 2
        service-template 1
    radio enable
#

```

- Switch 的配置文件:

```

#
vlan 100
#
vlan 200
#

```

```
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200
  port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 100
#
```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“二层技术配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“二层技术命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“ACL 和 QoS 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“ACL 和 QoS 命令参考”。

# WIDS 典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |    |
|------------------------|----|
| 1 简介.....              | 1  |
| 2 配置前提 .....           | 1  |
| 3 非法设备检测并反制配置举例.....   | 1  |
| 3.1 组网需求 .....         | 1  |
| 3.2 配置思路 .....         | 2  |
| 3.3 配置注意事项.....        | 2  |
| 3.4 配置步骤 .....         | 2  |
| 3.4.1 AC 的配置 .....     | 2  |
| 3.4.2 Switch 的配置 ..... | 4  |
| 3.5 验证配置 .....         | 5  |
| 3.6 配置文件 .....         | 5  |
| 4 黑白名单配置举例.....        | 7  |
| 4.1 组网需求 .....         | 7  |
| 4.2 配置思路 .....         | 7  |
| 4.3 配置注意事项.....        | 8  |
| 4.4 配置步骤 .....         | 8  |
| 4.4.1 AC 的配置 .....     | 8  |
| 4.4.2 Switch 的配置 ..... | 9  |
| 4.5 验证配置 .....         | 10 |
| 4.6 配置文件 .....         | 10 |
| 5 相关资料 .....           | 12 |

# 1 简介

本文介绍了 AC WIDS（Wireless Intrusion Detection System，无线入侵检测系统）特性的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WIDS 特性。

## 3 非法设备检测并反制配置举例

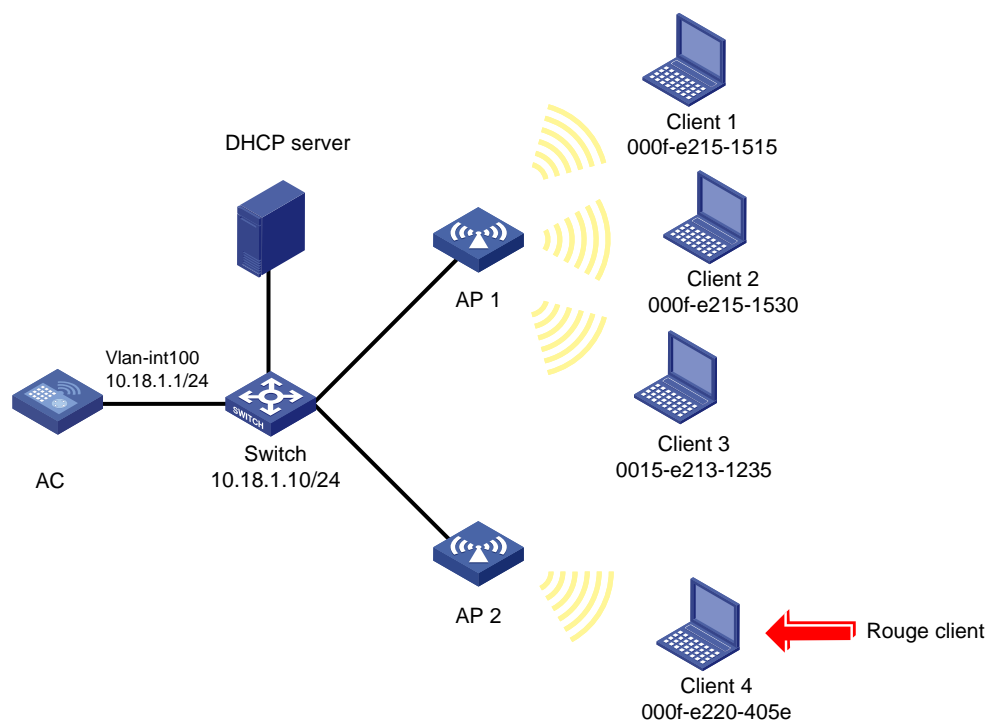
### 3.1 组网需求

如[图 1](#)所示，AP 1 和 AP 2 通过交换机连接 AC，AP 及 Client 通过 DHCP 服务器获取 IP 地址；现要求：

- AP 1 工作在 Normal 模式，为 Client 1、Client 2 和 Client 3 提供 WLAN 服务；
- AP 2 工作在 Monitor 模式，对非法设备进行检测；
- 禁止非法用户接入。



图1 WIDS 典型配置组网图



## 3.2 配置思路

为实现禁止非法用户接入，AC 上需要配置 Monitor 模式的 AP，并开启非法用户检测功能和反制功能。

## 3.3 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 AC 的配置

(1) 配置 AC 的接口

# 创建 VLAN100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。同时 VLAN100 也作为无线用户接入的 VLAN。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.18.1.1 24
[AC-Vlan-interface100] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，配置 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100
[AC-GigabitEthernet1/0/1] quit
```

# 创建编号为 1 的 WLAN-ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 100，禁止 VLAN 1 通过并允许 VLAN 100 不带 tag 通过。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 100
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 100 untagged
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

## (2) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID（服务模板的标识）为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 设置无线客户端接入该无线服务（SSID）的认证方式为开放式系统认证。

```
[AC-wlan-st-1] authentication-method open-system
```

# 使能服务模板。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

## (3) 配置 AP 1 为 Normal 模式，只提供 WLAN 服务

# 创建 AP 管理模板，其名称为 officeap1，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap1 model WA2620E-AGN
```

# 设置 AP 的序列号为 21023529G007C000020。

```
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
```

# 设置 radio2 的射频类型为 802.11g。

```
[AC-wlan-ap-officeap1] radio 2 type dot11g
```

# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联。

```
[AC-wlan-ap-officeap1-radio-2] service-template 1
[AC-wlan-ap-officeap1-radio-2] radio enable
[AC-wlan-ap-officeap1-radio-2] quit
[AC-wlan-ap-officeap1] quit
```

## (4) 配置 AP 2 的工作模式为 Monitor 模式

# 创建 AP 管理模板，其名称为 officeap2，型号名称选择 WA2620E-AGN。

```
[AC] wlan ap officeap2 model WA2620E-AGN
[AC-wlan-ap-officeap2] serial-id 21023529G007C000021
```

# 配置 AP 2 的工作模式为 Monitor 模式。

```
[AC-wlan-ap-officeap2] work-mode monitor
[AC-wlan-ap-officeap2] quit
```

#### (5) 配置 WIDS 规则

# 进入 WLAN IDS 视图。

```
[AC] wlan ids
```

# 将 Client1、Client2、Client3 的 MAC 地址添加到允许接入的 MAC 地址列表中。

```
[AC-wlan-ids] device permit mac-address 000f-e215-1515
[AC-wlan-ids] device permit mac-address 000f-e215-1530
[AC-wlan-ids] device permit mac-address 0015-e213-1235
```

# 将 Client4 的 MAC 地址添加到禁止接入的 MAC 地址列表中。

```
[AC-wlan-ids] device attack mac-address 0015-e220-405e
```

# 配置 AC 的反制模式，根据静态配置的禁止 MAC 地址列表进行反制。

```
[AC-wlan-ids] countermeasures mode config
```

# 使能反制功能。

```
[AC-wlan-ids] countermeasures enable
[AC-wlan-ids] quit
```

### 3.4.2 Switch 的配置

# 创建 VLAN 100，用于转发 AC 和 AP 间 LWAPP 隧道内的流量和无线用户的接入。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 通过。

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口属性为 Access，并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
```

```
[Switch-GigabitEthernet1/0/3] port access vlan 100
# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/3 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
# 配置 Switch 与 DHCP 服务器相连的 GigabitEthernet1/0/4 接口属性为 Access, 并允许 VLAN100 通过。
[Switch] interface gigabitethernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

### 3.5 验证配置

(1) 通过命令 **display wlan client** 查看上线的 Client。

```
<Sysname> display wlan client
Total Number of Clients          : 3
                                Client Information
                                SSID: office
-----
MAC Address   User Name          APID/RID IP Address          VLAN
-----
000f-e215-1515 Client 1          1/2      10.18.1.11            100
000f-e215-1530 Client 2          1/2      10.18.1.12            100
0015-e213-1235 Client 3          1/2      10.18.1.13            100
```

(2) Client 4 接入网络后马上断线, 再次接入网络后又断线, 如此反复, ping 其他设备有大量丢包

```
C:\Documents and Settings\Client 4> ping 10.18.1.1 -t
```

```
Pinging 10.18.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.18.1.10: bytes=32 time=1433ms TTL=255
Reply from 10.18.1.10: bytes=32 time=40ms TTL=255
Reply from 10.18.1.10: bytes=32 time=11ms TTL=255
Reply from 10.18.1.10: bytes=32 time=46ms TTL=255
Reply from 10.18.1.10: bytes=32 time=17ms TTL=255
Request timed out.
Request timed out.
```

### 3.6 配置文件

```
#
vlan 100
#
```

```

wlan service-template 1 clear
  ssid service
  bind WLAN-ESS 1
  service-template enable
#
interface Vlan-interface100
  ip address 10.18.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100
  port trunk pvid vlan 100
#
interface WLAN-ESS1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 100 untagged
  port hybrid pvid vlan 100
  mac-vlan enable
#
wlan ap officeap1 model WA2620E-AGN
serial-id 21023529G007C000020
  radio 2
    service-template 1
    radio enable
#
wlan ap officeap2 model WA2620E-AGN
serial-id 21023529G007C000021
  work-mode monitor
  radio 2
    radio enable
#
wlan ids
  countermeasures enable
  device attack mac-address 0015-e220-405e
  device permit mac-address 000f-e215-1515
  device permit mac-address 000f-e215-1530
  device permit mac-address 0015-e213-1235
#

```

- Switch

```

#
vlan 100
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100

```

```

port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/4
port link-type access
port access vlan 100
#

```

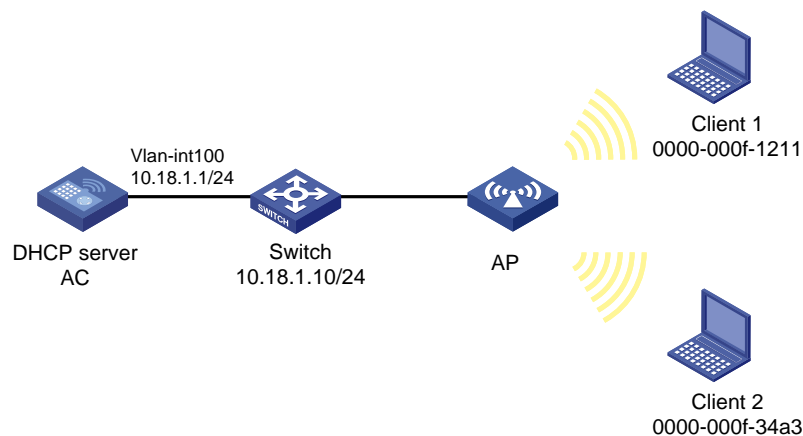
## 4 黑白名单配置举例

### 4.1 组网需求

如[图 2](#)所示，AP 通过交换机连接 AC，AC 作为 DHCP 服务器为 AP 和 Client 动态分配 IP 地址。具体应用需求如下：

- 任何来源于 Client 1 的帧将被过滤并丢弃；
- 所有来源于 Client 2 的帧将被保留做进一步处理；
- AC 启动攻击检测功能，任何攻击 AP 的设备将被加入到动态黑名单。

图2 黑白名单配置组网图



### 4.2 配置思路

为了防止外部非法用户访问内部网络，同时允许指定的人员访问内部网络，在 AC 上将无线客户端用户的 MAC 地址配置为静态黑名单（非法用户）、静态白名单（合法用户）。

## 4.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- 白名单的优先级高于黑名单，如果设置了白名单列表，则只有 AP 收到的 802.11 帧的源 MAC 在白名单内，该帧将被作为合法帧进一步处理，否则该帧被丢弃；如果没有设置白名单列表，则继续搜索静态和动态的黑名单列表进行处理。

## 4.4 配置步骤

### 4.4.1 AC 的配置

#### (1) 配置 AC 的接口

#创建 VLAN100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。同时 VLAN100 为无线用户接入的 VLAN。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.18.1.1 24
[AC-Vlan-interface100] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，当前 Trunk 口的 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 DHCP 服务

# 全局下使能 DHCP

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 0 动态分配的网段为 10.18.1.0/24。

```
[AC] dhcp server ip-pool 0
[AC-dhcp-pool-0] network 10.18.1.0 mask 255.255.255.0
[AC-dhcp-pool-0] quit
```

#### (3) 配置无线服务

# 创建编号为 1 的 WLAN-ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置端口的链路类型为 Hybrid。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 100，禁止 VLAN 1 通过并允许 VLAN 100 不带 tag 通过。

```
[AC-WLAN-ESS1] port hybrid pvid vlan 100
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 100 untagged
```

```

# 使能 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
# 创建 clear 类型的服务模板 1。
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service。
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 设置无线客户端接入该无线服务（SSID）的认证方式为开放式系统认证。
[AC-wlan-st-1] authentication-method open-system
# 使能服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit

```

#### (4) 配置 AP

```

# 创建 AP 管理模板，其名称为 officeap，型号名称这里选择 WA2620E-AGN。
[AC] wlan ap officeap model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 设置 radio2 的射频类型为 802.11g。
[AC-wlan-ap-officeap] radio 2 type dot11g
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行关联。
[AC-wlan-ap-officeap-radio-2] service-template 1
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] return

```

#### (5) 配置黑白名单

```

# 进入 WLAN IDS 视图。
[AC] wlan ids
# 添加 MAC 地址为 0000-000f-34a3 的客户端到白名单列表。
[AC-wlan-ids] whitelist mac-address 0000-000f-34a3
# 添加 MAC 地址为 0000-000f-1211 的客户端到黑名单列表。
[AC-wlan-ids] static-blacklist mac-address 0000-000f-1211
# 配置入侵检测功能，检测 flood，spoof，weak-iv 攻击。
[AC-wlan-ids] attack-detection enable all
[AC-wlan-ids] quit

```

### 4.4.2 Switch 的配置

```

# 创建 VLAN 100，用于转发 AC 和 AP 间 LWAPP 隧道内的流量和无线用户的接入。
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 口的 PVID 为 100，允许 VLAN 100 通过。

```



```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，当前 Access 口允许 VLAN100 通过。
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

## 4.5 验证配置

# 使用命令 **display wlan whitelist** 显示配置的黑名单列表。

```
[AC] display wlan whitelist
Total Number of Entries: 1

                                Whitelist
-----
MAC-Address
-----
0000-000f-34a3
-----
```

# 使用命令 **display wlan blacklist static** 显示配置的静态黑名单列表。

```
[AC] display wlan blacklist static
Total Number of Entries: 1

                                Static Blacklist
-----
MAC-Address
-----
0000-000f-1211
-----
```

## 4.6 配置文件

```
#
vlan 100
#
dhcp server ip-pool 0
network 10.18.1.0 mask 255.255.255.0
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
```

```

service-template enable
#
interface Vlan-interface100
ip address 10.18.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk permit vlan 100
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 100 untagged
port hybrid pvid vlan 100
mac-vlan enable
#
wlan ap officeap model WA2620E-AGN
serial-id 21023529G007C000020
radio 2
service-template 1
radio enable
#
wlan ids
static-blacklist mac-address 0000-000f-1211
whitelist mac-address 0000-000f-34a3
attack-detection enable all
#
dhcp enable
#

```

## - Switch

```

#
vlan 100
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#

```

## 5 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# WIPS 功能典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                          |    |
|--------------------------|----|
| 1 简介.....                | 1  |
| 2 配置前提 .....             | 1  |
| 3 配置举例 .....             | 1  |
| 3.1 组网需求 .....           | 1  |
| 3.2 配置思路 .....           | 2  |
| 3.3 配置注意事项.....          | 2  |
| 3.4 配置步骤 .....           | 2  |
| 3.4.1 WIPS AC 的配置.....   | 2  |
| 3.4.2 AC 的配置 .....       | 3  |
| 3.4.3 Switch A 的配置 ..... | 4  |
| 3.4.4 Switch B 的配置 ..... | 5  |
| 3.5 验证结果 .....           | 5  |
| 3.6 配置信息 .....           | 7  |
| 4 相关资料 .....             | 10 |

# 1 简介

本文档介绍用户通过配置 WIPS（Wireless Intrusion Prevention System，无线入侵防护）功能实现非法设备检测的配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

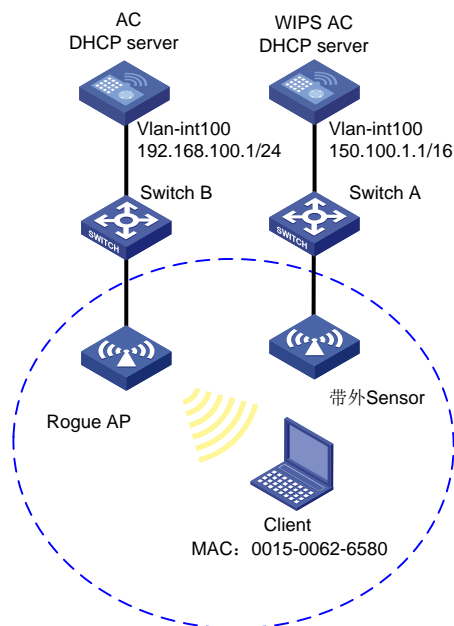
本文档假设您已了解 WIPS 的相关功能。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，WIPS AC 通过 Switch A 与 Sensor 相连，WIPS AC 作为 DHCP server 为 Sensor 分配 IP 地址，Client 关联的 Rogue AP 作为 Sensor 检测的对象。现要求：配置 WIPS 功能，使 Sensor 能够检测网络中是否存在 Rogue AP。

图1 WIPS 检测非法设备组网图



## 3.2 配置思路

为了使 AP 能够成为 WIPS 功能中的 Sensor，需要在 AP 的 radio 射频配置中将 WIPS 检测模式配置为带外模式。

## 3.3 配置注意事项

- WIPS 特性需要安装 License 才可使用。
- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.4 配置步骤

### 3.4.1 WIPS AC 的配置

#### (1) 配置 WIPS AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。WIPS AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<WIPS AC> system-view
[WIPS AC] vlan 100
[WIPS AC-vlan100] quit
[WIPS AC] interface Vlan-interface 100
[WIPS AC-Vlan-interface100] ip address 150.100.1.1 16
[WIPS AC-Vlan-interface100] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，当前 Trunk 口的 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 通过。

```
[WIPS AC] interface gigabitethernet 1/0/1
[WIPS AC-GigabitEthernet1/0/1] port link-type trunk
[WIPS AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[WIPS AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[WIPS AC-GigabitEthernet1/0/1] port trunk permit vlan 100
[WIPS AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 DHCP

# 在 WIPS AC 上开启 DHCP 服务。

```
[WIPS AC] dhcp enable
```

# 配置 DHCP 地址池 vlan100 为 AP 动态分配的网段为 150.100.0.0/16，网关地址为 150.100.1.1。

```
[WIPS AC] dhcp server ip-pool vlan100
[WIPS AC-dhcp-pool-vlan100] network 150.100.1.1 16
[WIPS AC-dhcp-pool-vlan100] gateway-list 150.100.1.1
[WIPS AC-dhcp-pool-vlan100] quit
```

#### (3) 配置 AP 作为带外 Sensor

# 创建型号为 WA2620E-AGN 的 AP 模板名为 officeap，指定其序列号。

```
[WIPS AC] wlan ap officeap model WA2620E-AGN
[WIPS AC-wlan-ap-officeap] serial-id 21023529G007C000020
```

# 在 AP 的 Radio1 上开启 WIPS 功能并采用带外 Sensor 模式，使能 AP 的 radio 1 射频。

```
[WIPS AC-wlan-ap-officeap] radio 1
[WIPS AC-wlan-ap-officeap-radio-1] wips detect mode detect-only
[WIPS AC-wlan-ap-officeap-radio-1] radio enable
[WIPS AC-wlan-ap-officeap-radio-1] return
```

#### (4) 配置 WIPS

# 进入 WIPS 视图。

```
[WIPS AC] wlan ips
```

# 配置自定义 AP 分类规则 **test**：当检测到 AP 使用的无线服务的 SSID 为 **service** 时，该 AP 会被归类为 **Rogue AP**。

```
[WIPS AC-wlan-ips] ap-classification-rule test
[WIPS AC-wlan-ips-class-test] sub-rule ssid case-sensitive equal service
[WIPS AC-wlan-ips-class-test] classify-type rogue-ap
[WIPS AC-wlan-ips-class-test] quit
```

# 配置 WIPS 虚拟安全域 **testvsd**。

```
[WIPS AC-wlan-ips] virtual-security-domain testvsd
```

# 将 **officeap** 添加到虚拟安全域 **testvsd**，并绑定自定义 AP 分类规则 **test**。

```
[WIPS AC-wlan-ips-vsd-testvsd] sensor officeap
[WIPS AC-wlan-ips-vsd-testvsd] ap-classification-rule test
[WIPS AC-wlan-ips-vsd-testvsd] quit
```

# 使能 WIPS 功能。

```
[WIPS AC-wlan-ips] wips enable
```

### 3.4.2 AC 的配置

#### (1) 配置 AC 的接口

# 创建 **VLAN 100** 及其对应的 **VLAN** 接口，并为该接口配置 **IP** 地址。**AC** 将使用该接口的 **IP** 地址与 **AP** 建立 **LWAPP** 隧道。同时 **VLAN100** 为无线用户接入的 **VLAN**。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.1 24
[AC-Vlan-interface100] quit
```

# 将与 **Switch** 相连的接口 **GigabitEthernet1/0/1** 的链路类型配置为 **Trunk**，配置 **PVID** 为 **100**，禁止 **VLAN1** 通过，允许 **VLAN 100** 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 DHCP

# 在 **AC** 上开启 **DHCP** 服务。

```
[AC] dhcp enable
```

# 配置 **DHCP** 地址池 **vlan100** 为 **AP** 动态分配的网段为 **192.168.1.0/24**，网关地址为 **192.168.1.1**。



```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 192.168.1.0 24
[AC-dhcp-pool-vlan100] gateway-list 192.168.1.1
[AC-dhcp-pool-vlan100] quit
```

### (3) 配置 WLAN-ESS 接口

# 创建 WLAN-ESS1 接口，并设置端口的链路类型为 Hybrid 类型。

```
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 100，禁止 VLAN 1 通过，允许 VLAN 100 不带 tag 通过。

```
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 100 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 100
```

# 使能 MAC VLAN 功能。

```
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
```

### (4) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC] wlan service-template 1 clear
```

# 设置当前服务模板的 SSID 为 service。

```
[AC-wlan-st-1] ssid service
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC-wlan-st-1] bind wlan-ess 1
```

# 启用无线服务。

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

# 创建型号为 WA2620E-AGN 的 AP 模板名为 rouge，指定其序列号。

```
[AC] wlan ap rouge model WA2620E-AGN
[AC-wlan-ap- rouge] serial-id 21023529G007C000021
```

# 在 AP 的 Radio1 上绑定服务模板，使能 AP 的 radio 1 射频。

```
[AC-wlan-ap-rouge] radio 1
[AC-wlan-ap-rouge-radio-1] service-template 1
[AC-wlan-ap-rouge-radio-1] radio enable
[AC-wlan-ap-rouge-radio-1] return
```

## 3.4.3 Switch A 的配置

# 创建 VLAN 100，用于转发 AC 和 AP 间 LWAPP 隧道内的流量。

```
<Switch A> system-view
[Switch A] vlan 100
[Switch A-vlan100] quit
```

# 配置 Switch A 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止 VLAN 1 通过，允许 VLAN 100 通过。

```
[Switch A] interface gigabitethernet1/0/1
[Switch A-GigabitEthernet1/0/1] port link-type trunk
[Switch A-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[Switch A-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch A-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch A-GigabitEthernet1/0/1] quit
```

# 配置 Switch A 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN100 通过。

```
[Switch A] interface gigabitethernet1/0/2
[Switch A-GigabitEthernet1/0/2] port link-type access
[Switch A-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch A 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch A-GigabitEthernet1/0/2] poe enable
[Switch A-GigabitEthernet1/0/2] quit
```

### 3.4.4 Switch B 的配置

# 创建 VLAN 100，用于转发 AC 和 AP 间 LWAPP 隧道内的流量和无线用户的接入。

```
<Switch B> system-view
[Switch B] vlan 100
[Switch B-vlan100] quit
```

# 配置 Switch B 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，配置 PVID 为 100，禁止 VLAN 1 通过，允许 VLAN 100 通过。

```
[Switch B] interface gigabitethernet1/0/1
[Switch B-GigabitEthernet1/0/1] port link-type trunk
[Switch A-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch B-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch B-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch B-GigabitEthernet1/0/1] quit
```

# 配置 Switch B 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```
[Switch B] interface gigabitethernet1/0/2
[Switch B-GigabitEthernet1/0/2] port link-type access
[Switch B-GigabitEthernet1/0/2] port access vlan 100
```

# 配置 Switch B 与 AP 相连的 GigabitEthernet1/0/2 接口使能 PoE 功能。

```
[Switch B-GigabitEthernet1/0/2] poe enable
[Switch B-GigabitEthernet1/0/2] quit
```

## 3.5 验证结果

- (1) 在 WIPS AC 上通过命令行 **display wlan ips device ap** 和命令 **display wlan ips device client** 查看检测到 Rogue AP 设备和 Unauthorized Client（在 Rogue AP 上线的 Client 按照 WIPS 的规则会被分类到 Unauthorized Client）设备。

```
[WIPS AC] display wlan ips devices ap
SL = severity level, #S = number of reporting sensors, S = status
VSD = virtual security domain, I = inactive, A = active
Cli = client, Chl = channel
```

Detected Wireless Devices

```
-----
MAC-Address      Type Classification      SL Last-Time              #S Chl S
-----
```

VSD default: 0

VSD testvsd: 1

|                |    |       |   |                     |   |    |   |
|----------------|----|-------|---|---------------------|---|----|---|
| 5866-ba20-6e61 | AP | Rogue | 0 | 2014-01-23/19:11:56 | 1 | 60 | A |
|----------------|----|-------|---|---------------------|---|----|---|

[WIPS AC] display wlan ips devices client

SL = severity level, #S = number of reporting sensors, S = status

VSD = virtual security domain, I = inactive, A = active

Cli = client, Chl = channel

Detected Wireless Devices

| MAC-Address | Type | Classification | SL | Last-Time | #S | Chl | S |
|-------------|------|----------------|----|-----------|----|-----|---|
|-------------|------|----------------|----|-----------|----|-----|---|

VSD default: 0

VSD testvsd: 1

|                |     |              |   |                     |   |    |   |
|----------------|-----|--------------|---|---------------------|---|----|---|
| 0015-0062-6580 | Cli | Unauthorized | - | 2014-01-23/19:14:14 | 1 | 60 | A |
|----------------|-----|--------------|---|---------------------|---|----|---|

- (2) 在 WIPS AC 上通过命令行 **display wlan ips device ap rogue verbose** 可以查看 Rogue AP 的详细信息，该 AP 的 SSID 为 service。

[WIPS AC] display wlan ips devices ap rogue verbose

Detected Wireless Devices

VSD: default

Total Number of APs: 0

VSD: testvsd

Total Number of APs: 1

BSSID : 5866-ba20-6e61

Vendor: Hangzhou H3C Technologies Co., Limited

|                        |                       |
|------------------------|-----------------------|
| SSID                   | : service             |
| Status                 | : Active              |
| Classification         | : Rogue               |
| Severity Level         | : 0                   |
| Security               | : Clear               |
| Encrypt Method         | : -NA-                |
| Authentication Method  | : None                |
| Radio Type             | : 802.11an            |
| Channel                | : 60                  |
| In Countermeasure List | : No                  |
| Up Time                | : 2014-01-23/17:44:25 |
| First Reported Time    | : 2014-01-23/17:44:26 |
| Last Reported Time     | : 2014-01-23/19:15:07 |
| Reporting Sensor       | : 1                   |
| Sensor 1               | : officeap            |
| RadioId                | : 1                   |
| RSSI                   | : 22                  |
| Last Reported Time     | : 2014-01-23/19:15:07 |
| Attached Clients       | : 1                   |
| Client 1               | : 0015-0062-6580      |

- (3) 在 WIPS AC 上通过命令行 **display wlan ips device client unauthorized verbose** 查看该未授权 Client 的详细信息。

```
[WIPS AC] display wlan ips devices client unauthorized verbose
Detected Wireless Devices
```

```
VSD: default
Total Number of Clients: 0
```

```
VSD: testvsd
Total Number of Clients: 1
```

```
MAC Address: 0015-0062-6580
Vendor: Intel Corporate
BSSID           : 5866-ba20-6e61
Status          : Active
State           : Association
Classification   : Unauthorized
RadioType       : 802.11an
Channel         : 60
In Countermeasure List : No
First Reported Time   : 2014-01-23/17:57:11
Last Reported Time    : 2014-01-23/19:18:50
Reporting Sensor     : 1
Sensor 1           : officeap
  RadioId          : 1
  RSSI             : 21
  Last Reported Time : 2014-01-23/19:18:50
```

## 3.6 配置信息

- WIPS AC

```
#
vlan 100
#
dhcp server ip-pool vlan100
network 150.100.0.0 mask 255.255.0.0
gateway-list 150.100.1.1
#
interface Vlan-interface100
ip address 150.100.1.1 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk pvid vlan 100
```

```

port trunk permit vlan 100
#
wlan ap officeap model WA2620E-AGN id 1
  serial-id 21023529G007C000020
  radio 1
    wips detect mode detect-only
    radio enable
  radio 2
#
wlan ips
  wips enable
  malformed-detect-policy default
  signature deauth_flood signature-id 1
  signature broadcast_deauth_flood signature-id 2
  signature disassoc_flood signature-id 3
  signature broadcast_disassoc_flood signature-id 4
  signature eapol_logoff_flood signature-id 5
  signature eap_success_flood signature-id 6
  signature eap_failure_flood signature-id 7
  signature pspoll_flood signature-id 8
  signature cts_flood signature-id 9
  signature rts_flood signature-id 10
  signature-policy default
  countermeasure-policy default
  attack-detect-policy default
  ap-classification-rule test
    classify-type rogue-ap
    sub-rule ssid case-sensitive equal service
  virtual-security-domain default
    attack-detect-policy default
    malformed-detect-policy default
    signature-policy default
    countermeasure-policy default
  virtual-security-domain testvsd
    attack-detect-policy default
    malformed-detect-policy default
    signature-policy default
    countermeasure-policy default
  ap-classification-rule test precedence 0
  sensor officeap
#
  dhcp enable
#
•   AC
#
vlan 200
#
dhcp server ip-pool vlan100

```

```

network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.1
#
wlan service-template 1 clear
ssid service
bind WLAN-ESS 1
service-template enable
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap rouge model WA2620E-AGN id 1
serial-id 21023529G007C000021
radio 1
service-template 1
radio enable
radio 2
#
dhcp enable
#

```

#### ● Switch A

```

#
vlan 100
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
poe enable
#

```

#### ● Switch B

```

#
vlan 100
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100

```

```
port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# Telnet 访问控制典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。



# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置步骤 .....         | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 2 |
| 3.4 验证配置 .....         | 2 |
| 3.5 配置文件 .....         | 3 |
| 4 相关资料 .....           | 3 |

# 1 简介

本文介绍使用访问控制列表和 IP Source Guard 功能控制远程 Telnet 无线控制器的典型配置案例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

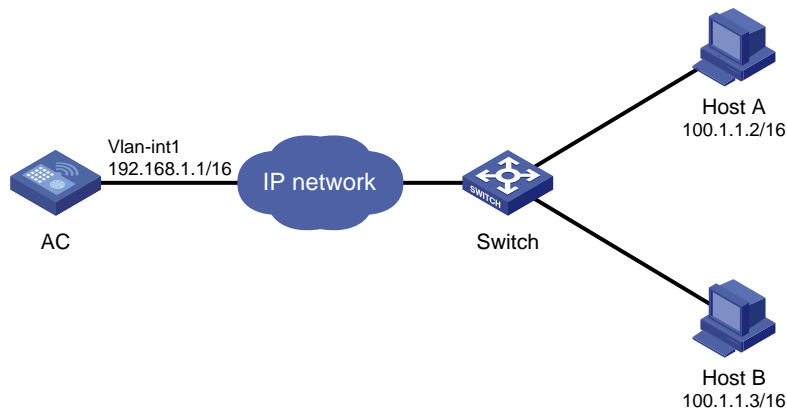
本文档假设您已了解 Telnet、ACL 和 IP Source Guard 特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，两台主机到 AC 路由可达。通过在 AC 上配置 ACL 功能以实现：仅允许 Host A 通过 Telnet 登录 AC，不允许 Host B 通过 Telnet 登录 AC。

图1 基于 AC 的 Telnet 访问控制组网图



### 3.2 配置思路

- 为了实现仅允许 Host A 可以通过 Telnet 方式登录 AC，需要通过 ACL 来匹配 Host A 的 IP 地址，并在 AC 的 VTY 用户线视图下使用该 ACL 对 Telnet 客户端进行限制。
- 为了防止其它主机使用 Host A 的 IP 地址 Telnet 登录 AC，需要在 Switch 上配置全局静态绑定表项，将 Host A 的 IP 地址和 MAC 地址进行绑定。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 ACL

# 创建一个编号为 2000 的基本 ACL，并进入其视图。

```
<AC> system-view
```

```
[AC] acl number 2000
```

# 创建规则仅允许来自 100.1.1.2/16 主机的报文通过。

```
[AC-acl-basic-2000] rule 0 permit source 100.1.1.2 0
```

```
[AC-acl-basic-2000] quit
```

#### (2) 将 ACL 应用到 VTY 用户界面

# 进入 VTY 0~4 用户界面视图。

```
[AC] user-interface vty 0 4
```

```
[AC-ui-vty0-4] acl 2000 inbound
```

```
[AC-ui-vty0-4] quit
```

# 启动 Telnet 服务。

```
[AC] telnet server enable
```

### 3.3.2 Switch 的配置

# 配置全局 IPv4 静态绑定表项，绑定 IP 地址 100.1.1.2 和 MAC 地址 0001-0203-0405。

```
[Switch] ip source binding ip-address 100.1.1.2 mac-address 0001-0203-0405
```

## 3.4 验证配置

# 使用 **display ip source binding** 命令显示 IPv4 绑定表项信息。

```
[Switch] display ip source binding
```

```
Total entries found: 1
```

| MAC Address    | IP Address | VLAN | Interface | Type   |
|----------------|------------|------|-----------|--------|
| 0001-0203-0405 | 100.1.1.2  | N/A  | N/A       | Static |

# Host A 通过 Telnet 远程登录到 AC，在 AC 的视图下观察到访问成功。

```
#Nov 20 11:15:17:407 2013 AC SHELL/4/LOGIN: Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1<hh3cLogIn>: login from VTY
```

```
%Nov 20 11:15:17:428 2013 AC SHELL/5/SHELL_LOGIN: VTY logged in from 100.1.1.2.
```

# Host B 通过 Telnet 远程登录 AC，在 Telnet 远程登录视图下，观察到 Host B 登录 AC 失败。

# 使用 **display acl** 命令显示全部 ACL 的配置和运行情况。

```
<AC> display acl 2000
```

```
Basic ACL 2000, named -none-, 1 rule,
```

```
ACL's step is 5
```

```
rule 0 permit source 100.1.1.2 0
```

# 使用 **display users all** 命令显示当前正在使用的用户界面的相关信息。

```
<AC> display users all
```

```
The user application information of all user interfaces:
```

| Idx | UI | Delay | Type     | Userlevel |
|-----|----|-------|----------|-----------|
| +   | 0  | CON 0 | 00:00:00 | 3         |

```
7    AUX 0
+ 8    VTY 0    00:00:05 TEL  3
9    VTY 1
10   VTY 2
11   VTY 3
12   VTY 4
```

Following are more details.

VTY 0 :

Location: 100.1.1.2

+ : User-interface is active.

F : User-interface is active and work in async mode.

## 3.5 配置文件

- AC:

```
#
telnet server enable
#
acl number 2000
rule 0 permit source 100.1.1.2 0
#
user-interface vty 0 4
acl 2000 inbound
authentication-mode none
#
```

- Switch:

```
#
ip source binding ip-address 100.1.1.2 mac-address 0001-0203-0405
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“ACL 和 QoS 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“ACL 和 QoS 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“基础配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“基础命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# 基于 IPv6 的 Telnet 访问控制典型配置举例 (V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置思路 .....         | 1 |
| 3.3 配置步骤 .....         | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 2 |
| 3.4 验证配置 .....         | 2 |
| 3.5 配置文件 .....         | 3 |
| 4 相关资料 .....           | 3 |

# 1 简介

本文介绍使用访问控制列表和 IP Source Guard 功能控制远程 Telnet 无线控制器的典型配置案例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

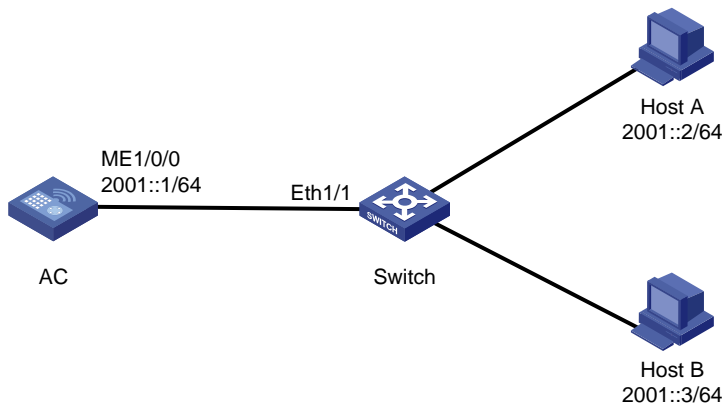
本文档假设您已了解 Telnet、ACL 和 IP Source Guard 特性。

## 3 配置举例

### 3.1 组网需求

如图 1 所示，两台主机到 AC 路由可达。通过在 AC 上配置 ACL 功能以实现：仅允许 Host A 通过 Telnet 登录 AC，不允许 Host B 通过 Telnet 登录 AC。

图1 基于 IPv6 的 Telnet 访问控制组网图



### 3.2 配置思路

- 为了实现仅允许 Host A 可以通过 Telnet 方式登录 AC，需要通过 ACL 来匹配 Host A 的 IPv6 地址，并在 AC 的 VTY 用户线视图下使用该 ACL 对 Telnet 客户端进行限制。
- 为了防止其它主机使用 Host A 的 IPv6 地址 Telnet 登录 AC，需要在 Switch 上配置全局静态绑定表项，将 Host A 的 IPv6 地址和 MAC 地址进行绑定。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 ACL

# 创建一个基于 IPv6 编号为 2000 的基本 ACL，并进入其视图。

```
<AC> system-view
[AC] acl ipv6 number 2000
# 创建规则仅允许来自 2001::2 主机的报文通过。
[AC-acl6-basic-2000] rule 0 permit source 2001::2 128
[AC-acl6-basic-2000] quit
```

#### (2) 将 ACL 应用到 VTY 用户界面

# 进入 VTY 0~4 用户界面视图。

```
[AC] user-interface vty 0 4
[AC-ui-vty0-4] acl ipv6 2000 inbound
[AC-ui-vty0-4] quit
# 启动 Telnet 服务。
[AC] telnet server enable
```

### 3.3.2 Switch 的配置

# 在二层以太网端口 Ethernet1/1 上配置对报文的源 IP 地址绑定功能，并在端口上配置一条 IPv6 静态绑定表项。

```
<Switch> system-view
[Switch] interface ethernet 1/1
[Switch-Ethernet1/1] ipv6 verify source ipv6-address
[Switch-Ethernet1/1] ipv6 source binding ipv6-address 2001::2 mac-address 6805-CA21-DDA0
[Switch-Ethernet1/1] quit
```

## 3.4 验证配置

# 使用 **display ipv6 source binding** 命令显示 IPv6 绑定表项信息。

```
[Switch] display ipv6 source binding
Total entries found: 1
MAC Address          IPv6 Address          VLAN      Interface      Type
6805-CA21-DDA0       2001::2               N/A       N/A            Static
```

# Host A 通过 Telnet 远程登录 AC，在 AC 的视图下观察到访问成功。

```
#Aug 16 17:34:36:182 2018 AC SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1<hh3cLogIn>: login from VTY
%Aug 16 17:34:36:183 2018 AC SHELL/5/SHELL_LOGIN: VTY logged in from 2001::2.
```

# Host B 通过 Telnet 远程登录 AC，观察到 Host B 登录 AC 失败。

# 使用 **display acl** 命令显示全部 ACL 的配置和运行情况。

```
<AC> display acl ipv6 2000
Basic IPv6 ACL 2000, named -none-, 1 rule,
ACL's step is 5
rule 0 permit source 2001::2/128 (5 times matched)
```



# 使用 **display users all** 命令显示当前正在使用的用户界面的相关信息。

```
<AC> display users all
```

The user application information of all user interfaces:

| Idx | UI    | Delay    | Type | Userlevel |
|-----|-------|----------|------|-----------|
| 0   | CON   | 0        |      |           |
| + 1 | VTY 0 | 00:00:10 | TEL  | 3         |
| 2   | VTY 1 |          |      |           |
| 3   | VTY 2 |          |      |           |
| 4   | VTY 3 |          |      |           |
| 5   | VTY 4 |          |      |           |

Following are more details.

VTY 0 :

Location: 2001::2

+ : User-interface is active.

F : User-interface is active and work in async mode.

## 3.5 配置文件

- AC:

```
#
telnet server enable
#
acl ipv6 number 2000
rule 0 permit source 2001::2/128
#
interface M-Ethernet1/0/0
ipv6 address 2001::1/64
#
user-interface vty 0 4
acl ipv6 2000 inbound
#
```

- Switch:

```
#
interface Ethernet1/1
ipv6 verify source ipv6-address
ipv6 source binding ipv6-address 2001::2 mac-address 6805-CA21-DDA0
#
```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“ACL 和 QoS 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“ACL 和 QoS 命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“基础配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“基础命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“安全配置指导”。

- 《H3C 无线控制器产品 命令参考》中的“安全命令参考”。

# Rogue AP 检测功能典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                        |   |
|------------------------|---|
| 1 简介.....              | 1 |
| 2 配置前提 .....           | 1 |
| 3 配置举例 .....           | 1 |
| 3.1 组网需求 .....         | 1 |
| 3.2 配置注意事项.....        | 1 |
| 3.3 配置步骤.....          | 2 |
| 3.3.1 AC 的配置 .....     | 2 |
| 3.3.2 Switch 的配置 ..... | 4 |
| 3.4 验证配置 .....         | 5 |
| 3.5 配置文件 .....         | 6 |
| 4 相关资料 .....           | 7 |

# 1 简介

本文介绍了 Rogue AP 检测及反制特性的典型配置举例。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 Rogue AP 检测及反制特性。

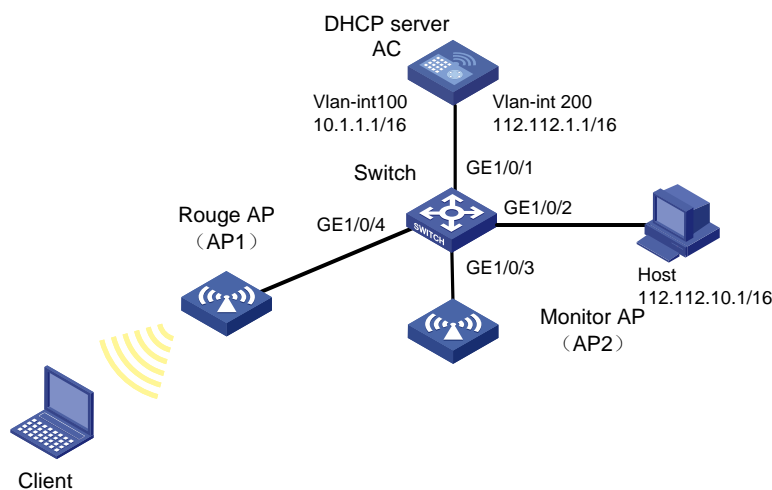
## 3 配置举例

### 3.1 组网需求

如图 1 所示，AP 通过交换机与 AC 相连，AC 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址，开启 Rogue AP 反制功能，以保证用户能通过合法的 AP 接入到正确的网络中，具体要求如下：

- Monitor AP 周期性的监听无线射频接口报文；
- 当发现 Rogue AP 时，Monitor AP 发起反制。

图1 Rogue AP 检测配置举例组网图



### 3.2 配置注意事项

配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

## 3.3 配置步骤

### 3.3.1 AC 的配置

#### (1) 配置 AC 的接口

# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.1.1.1 255.255.0.0
[AC-Vlan-interface100] quit
```

# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN 和无线用户接入的 VLAN。

```
[AC] vlan 200
[AC-vlan200] quit
```

# 进入 Vlan-interface200 的接口视图，配置 IP 地址为 112.112.1.1/16。

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 112.112.1.1 255.255.0.0
[AC-Vlan-interface200] quit
```

# 将与 Switch 相连的接口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，当前 Trunk 口的 PVID 为 100，禁止 VLAN1 通过，允许 VLAN 100 和 Client 使用的 VLAN200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

#### (2) 配置 DHCP 服务

# 开启 DHCP 服务。

```
[AC] dhcp enable
```

# 配置 DHCP 地址池 1 为 AP 动态分配的网段为 112.0.0.0/16。

```
[AC] dhcp server ip-pool 1
[AC-dhcp-pool-1] network 112.0.0.0 mask 255.255.0.0
[AC-dhcp-pool-1] quit
```

# 配置 DHCP 地址池 2 为 Client 动态分配的网段为 10.1.0.0/16。

```
[AC] dhcp server ip-pool 2
[AC-dhcp-pool-2] network 10.1.0.0 mask 255.255.0.0
[AC-dhcp-pool-2] quit
```

#### (3) 配置无线服务

# 创建编号为 1 的 WLAN-ESS 接口。

```
[AC] interface wlan-ess 1
```

# 配置 WLAN-ESS1 接口类型为 Hybrid 类型。

```
[AC-WLAN-ESS1] port link-type hybrid
```

# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 tag 通过。

```

[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 untagged
[AC-WLAN-ESS1] port hybrid pvid vlan 200
# 使能 MAC VLAN 功能。
[AC-WLAN-ESS1] mac-vlan enable
[AC-WLAN-ESS1] quit
# 创建一个新的服务模板（明文模板）1。
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service1。
[AC-wlan-st-1] ssid service1
# 将 WLAN-ESS1 接口绑定到服务模板 1。
[AC-wlan-st-1] bind wlan-ess 1
# 设置无线客户端接入该无线服务（SSID）的认证方式为开放式系统认证。
[AC-wlan-st-1] authentication-method open-system
# 使能服务模板。
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
(4) 配置 AP 1 为 Normal 模式，只提供 WLAN 服务
# 创建一个 AP 管理模板，其名称为 officeap1，型号名称为 WA2620E-AGN。
[AC] wlan ap officeap1 model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020。
[AC-wlan-ap-officeap1] serial-id 21023529G007C000020
# 设置 radio2 的射频类型为 802.11g。
[AC-wlan-ap-officeap1] radio 2 type dot11g
# 将服务模板 1 映射到射频 2。
[AC-wlan-ap-officeap1-radio-2] service-template 1
# 启用 AP 的 radio 2。
[AC-wlan-ap-officeap1-radio-2] radio enable
[AC-wlan-ap-officeap1-radio-2] quit
[AC-wlan-ap-officeap1] quit
(5) 配置 AP 2 为 monitor 模式
# 创建一个 AP 管理模板，其名称为 officeap2，型号名称为 WA2620E-AGN。
[AC] wlan ap officeap2 model WA2620E-AGN
[AC-wlan-ap-officeap2] serial-id 21023529G007C000021
# 配置 AP2 的工作模式为 monitor 模式。
[AC-wlan-ap-officeap2] work-mode monitor
[AC-wlan-ap-officeap2] radio 2
# 启用 AP 的 radio 2。
[AC-wlan-ap-officeap2-radio-2] radio enable
[AC-wlan-ap-officeap2-radio-2] quit
[AC-wlan-ap-officeap2] quit
(6) 配置 Rogue AP 检测及反制
# 进入 WLAN IDS 视图。
[AC] wlan ids

```

# 将 service 的这个 SSID 添加到允许 SSID 列表。

```
[AC-wlan-ids] device permit ssid service
```

# 使能反制 Rogue 设备的功能。

```
[AC-wlan-ids] countermeasures enable
```

# 对攻击列表里的所有 Rogue 设备进行反制。

```
[AC-wlan-ids] countermeasures mode all
```

```
[AC-wlan-ids] quit
```

### 3.3.2 Switch 的配置

# 创建 VLAN 100 和 VLAN 200, 其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量, VLAN 200 为无线用户接入的 VLAN。

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk, 配置 PVID 为 100,, 禁止 VLAN1 通过, 允许 VLAN 100 和 VLAN 200 通过。

```
[Switch] interface gigabitethernet1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置 Switch 与 Host 相连的 GigabitEthernet1/0/2 接口属性为 Access, 并允许 VLAN200 通过。

```
[Switch] interface gigabitethernet1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 200
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/3 接口属性为 Access, 并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/3
```

```
[Switch-GigabitEthernet1/0/3] port link-type access
```

```
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

# 配置 Switch 与 AP 1 相连的 GigabitEthernet1/0/3 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/3] poe enable
```

```
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/4 接口属性为 Access, 并允许 VLAN100 通过。

```
[Switch] interface gigabitethernet1/0/4
```

```
[Switch-GigabitEthernet1/0/4] port link-type access
```

```
[Switch-GigabitEthernet1/0/4] port access vlan 100
```

# 配置 Switch 与 AP 2 相连的 GigabitEthernet1/0/4 接口使能 PoE 功能。

```
[Switch-GigabitEthernet1/0/4] poe enable
```

```
[Switch-GigabitEthernet1/0/4] quit
```



## 3.4 验证配置

(1) 通过命令 **display wlan ids attack-list all** 查看 Monitor AP 发现的 Rouge AP。

```
[AC] display wlan ids attack-list all
Total Number of Entries: 1
Flags: a = adhoc, w = ap, c = client
#AP = number of active APs detecting, Ch = channel number
Attack List - All
-----
MAC Address      type #AP  Ch  Last Detected Time  SSID
-----
5866-ba71-38b0 r-w-  1    6   2014-01-04/17:10:43 "service1"
-----
```

其中 Type 前面有 r 的表示是 Rogue 设备。

(2) Client 试图通过 Rogue AP 和 Host 通信，启用反制功能前，Client 和 Host 可以正常通信。

```
C:\Documents and Settings\host>ping 112.112.10.1

Pinging 112.112.10.1 with 32 bytes of data:
Reply from 112.112.10.1: bytes=32 time=1ms TTL=128
Reply from 112.112.10.1: bytes=32 time=31ms TTL=128
Reply from 112.112.10.1: bytes=32 time<1ms TTL=128
Reply from 112.112.10.1: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 112.112.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 31ms, Average = 8ms
```

(3) Client 试图通过 Rogue AP 和 Host 通信，但启用反制功能后，Client 和 Host 的通信时断时续。

```
C:\Documents and Settings\host>ping 112.112.10.1 -t

Pinging 112.112.10.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 112.112.10.1: bytes=32 time=1433ms TTL=128
Reply from 112.112.10.1: bytes=32 time=40ms TTL=128
Reply from 112.112.10.1: bytes=32 time=11ms TTL=128
Reply from 112.112.10.1: bytes=32 time=46ms TTL=128
Reply from 112.112.10.1: bytes=32 time=17ms TTL=128
Request timed out.
Request timed out.
```

## 3.5 配置文件

- AC

```
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 1
network 112.0.0.0 mask 255.255.0.0
#
dhcp server ip-pool 2
network 10.1.0.0 mask 255.255.0.0
#
wlan service-template 1 clear
ssid service1
bind WLAN-ESS 1
authentication-method open-system
service-template enable
#
interface Vlan-interface100
ip address 10.1.1.1 255.255.0.0
#
interface Vlan-interface200
ip address 112.112.1.1 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk pvid vlan 100
port trunk permit vlan 100 200
#
interface WLAN-ESS1
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 200 untagged
port hybrid pvid vlan 200
mac-vlan enable
#
wlan ap officeap1 model WA2620E-AGN
serial-id 21023529G007C000020
radio 2 type 11g
radio enable
#
wlan ap officeap2 model WA2620E-AGN
serial-id 21023529G007C000021
work-mode monitor
radio 2 type 11g
```

```

        radio enable
#
wlan ids
    countermeasures enable
    device permit ssid service
#
    dhcp enable
#
    • Switch
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 200
#
interface GigabitEthernet1/0/3
    port link-type access
    port access vlan 100
    poe enable
#
interface GigabitEthernet1/0/4
    port link-type access
    port access vlan 100
    poe enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。

# VIP 通道典型配置举例(V5)

资料版本：6W114-20210416

---

Copyright ©2008-2021 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

# 目 录

|                      |   |
|----------------------|---|
| 1 简介.....            | 1 |
| 2 配置前提 .....         | 1 |
| 3 配置举例 .....         | 1 |
| 3.1 组网需求 .....       | 1 |
| 3.2 配置思路 .....       | 2 |
| 3.3 配置注意事项 .....     | 2 |
| 3.4 配置步骤 .....       | 2 |
| 3.4.1 AC 1 的配置 ..... | 2 |
| 3.4.2 AC 2 的配置 ..... | 4 |
| 3.5 验证配置 .....       | 5 |
| 3.6 配置文件 .....       | 5 |
| 4 相关资料 .....         | 6 |

# 1 简介

本文介绍了使用 IACTP 隧道配置 AC 间 VIP 通道的典型配置举例。

无线控制器支持 VIP 通道，VIP 通道用于完全隔离无线客户端。当无线客户端连接上 Guest SSID 之后，无线客户端的所有流量都会通过 IACTP 隧道（Inter Access Controller Tunneling Protocol 访问控制器间隧道协议）技术定向到 Internet，无线客户端可访问企业指定的网络资源，但无法访问任何企业内部资源，从根本上避免了来自企业内部的无线客户端造成的网络安全威胁。

## 2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

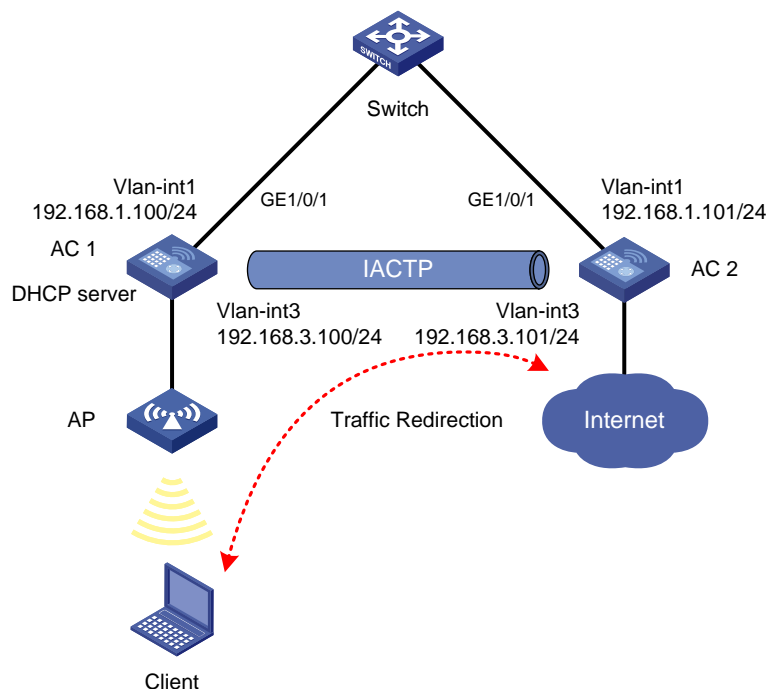
本文档假设您已了解 IACTP 隧道的特性。

## 3 配置举例

### 3.1 组网需求

如[图 1](#)所示，Client 通过无线网络访问 Internet，在 AC 1 上配置 DHCP 服务器，为 AP 和 Client 分配地址。现要求：在 AC 1 和 AC 2 间建立 IACTP 隧道，Client 通过 IACTP 隧道访问 Internet。

图1 AC 间 VIP 通道组网图



## 3.2 配置思路

为了使 AC 间建立 IACTP 隧道，需要在 AC 上分别配置源地址和成员地址建立隧道，使得 Client 能够通过 IACTP 隧道访问 Internet。

## 3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。
- Switch 上连接 AC 的两个端口需要具有相同的缺省 VLAN，并且均允许该缺省 VLAN 通过，因此在这两个端口上只要保持缺省配置即可。

## 3.4 配置步骤

### 3.4.1 AC 1 的配置

(1) 配置 AC 接口

# 配置 GigabitEthernet1/0/1 为 Hybrid 类型。

```
<AC1> system-view
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type hybrid
[AC1-GigabitEthernet1/0/1] port hybrid vlan 1 untagged
[AC1-GigabitEthernet1/0/1] quit
```

# 配置 VLAN 1 接口的 IP 地址。

```
[AC1] interface vlan-interface 1
[AC1-Vlan-interface1] ip address 192.168.1.100 255.255.255.0
[AC1-Vlan-interface1] quit
```

# 创建 VLAN 3，并配置 VLAN 3 接口的 IP 地址。

```
[AC1] vlan 3
[AC1-vlan3] quit
[AC1] interface vlan-interface 3
[AC1-Vlan-interface3] ip address 192.168.3.100 255.255.255.0
[AC1-Vlan-interface3] quit
```

# 创建 WLAN-ESS 1 接口，并进入该视图。

```
[AC1] interface wlan-ess 1
```

# 配置接口的链路类型为 Hybrid。

```
[AC1-WLAN-ESS1] port link-type hybrid
```

# 配置接口允许 VLAN 1 报文不带 VLAN tag。

```
[AC1-WLAN-ESS1] port hybrid vlan 1 untagged
```

# 使能 WLAN-ESS1 接口的 MAC VLAN 功能。

```
[AC1-WLAN-ESS1] mac-vlan enable
```

```
[AC1-WLAN-ESS1] quit
```

## (2) 配置 DHCP 服务

# 使能 DHCP 服务。

```
[AC] dhcp enable
```

# 创建名为 vlan1 的 DHCP 地址池，配置地址池范围为 192.168.1.200~192.168.1.250，网关地址为 192.168.1.100。

```
[AC] dhcp server ip-pool vlan1
[AC-dhcp-pool-vlan1] network ip range 192.168.1.200 192.168.1.250
[AC-dhcp-pool-vlan1] network mask 255.255.255.0
[AC-dhcp-pool-vlan1] gateway-list 192.168.1.100
[AC-dhcp-pool-vlan1] quit
```

## (3) 配置无线服务

# 创建 clear 类型的服务模板 1。

```
[AC1] wlan service-template 1 clear
```

# 设置服务模板 1 的 SSID（服务模板的标识）为 office。

```
[AC1-wlan-st-1] ssid office
```

# 将 WLAN-ESS1 接口绑定到服务模板 1。

```
[AC1-wlan-st-1] bind wlan-ess 1
```

# 开启服务模板 1 无线服务。

```
[AC1-wlan-st-1] service-template enable
```

```
[AC1-wlan-st-1] quit
```

## (4) 配置射频接口并绑定服务模板

# 创建 AP 管理模板 ap1，型号名称为 WA2620E-AGN，并配置序列号 210235A29G007C000020。

```
[AC1] wlan ap ap1 model WA2620E-AGN
[AC1-wlan-ap-ap1] serial-id 210235A29G007C000020
```



# 进入 AP 的 radio 1 射频视图，将 radio 1 绑定到服务模板 1，设置绑定到射频接口的 VLAN 编号为 VLAN 3。

```
[AC1-wlan-ap-ap1] radio 1
[AC1-wlan-ap-ap1-radio-1] service-template 1 vlan-id 3
```

# 使能 AP 的 radio 1。

```
[AC1-wlan-ap-ap1-radio-1] radio enable
[AC1-wlan-ap-ap1-radio-1] quit
[AC1-wlan-ap-ap1] quit
```

#### (5) 配置 IACTP 隧道

# 创建 IACTP 隧道 systemgroup，配置源 IP 地址为 192.168.1.100。

```
[AC1] wlan mobility-group systemgroup
[AC1-wlan-mg-systemgroup] source ip 192.168.1.100
```

# 配置 IACTP 隧道成员地址为 192.168.1.101，指定 IACTP 隧道的所在的 VLAN 为 VLAN 3。

```
[AC1-wlan-mg-systemgroup] member ip 192.168.1.101 vlan 3
```

# 开启 IACTP 隧道。

```
[AC1-wlan-mg-systemgroup] mobility-group enable
[AC1-wlan-mg-systemgroup] quit
```

### 3.4.2 AC 2 的配置

#### (1) 配置 AC 接口

# 配置 GigabitEthernet 1/0/1 为 Hybrid 类型。

```
<AC2> system-view
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type hybrid
[AC2-GigabitEthernet1/0/1] port hybrid vlan 1 untagged
[AC2-GigabitEthernet1/0/1] quit
```

# 配置 VLAN 1 接口的 IP 地址。

```
[AC2] interface vlan-interface 1
[AC2-Vlan-interface1] ip address 192.168.1.101 255.255.255.0
[AC2-Vlan-interface1] quit
```

# 创建 VLAN 3，并配置 VLAN 3 接口的 IP 地址。

```
[AC2] vlan 3
[AC2-vlan3] quit
[AC2] interface vlan-interface 3
[AC2-Vlan-interface3] ip address 192.168.3.101 255.255.255.0
[AC2-Vlan-interface3] quit
```

#### (2) 配置 IACTP 隧道

# 创建 IACTP 隧道 systemgroup，并配置源 IP 地址为 192.168.1.101。

```
[AC2] wlan mobility-group systemgroup
[AC2-wlan-mg-systemgroup] source ip 192.168.1.101
```

# 配置 IACTP 隧道成员地址为 192.168.1.100，指定 IACTP 隧道所在的 VLAN 为 VLAN 3。

```
[AC2-wlan-mg-systemgroup] member ip 192.168.1.100 vlan 3
```

# 开启 IACTP 隧道。

```
[AC2-wlan-mg-systemgroup] mobility-group enable
[AC2-wlan-mg-systemgroup] quit
```

### 3.5 验证配置

# 在 Client 上 ping AC 2 的 VLAN 3 接口 IP 地址 192.168.3.101，能够 ping 通。

```
C:\Documents and Settings\Administrator> ping 192.168.3.101
```

```
Pinging 192.168.3.101 with 32 bytes of data:
Reply from 192.168.3.101: bytes=32 time=2 ms ttl=127
Reply from 192.168.3.101: bytes=32 time=1 ms ttl=127
Reply from 192.168.3.101: bytes=32 time=1 ms ttl=127
Reply from 192.168.3.101: bytes=32 time=1 ms ttl=127
```

```
Ping statistics for 192.168.3.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

### 3.6 配置文件

- AC 1:

```
#
vlan 3
#
dhcp server ip-pool vlan1
network ip range 192.168.1.200 192.168.1.250
network mask 255.255.255.0
gateway-list 192.168.1.100
#
wlan service-template 1 clear
ssid office
bind WLAN-ESS 1
service-template enable
#
interface Vlan-interface1
ip address 192.168.1.100 255.255.255.0
#
interface Vlan-interface3
ip address 192.168.3.100 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 1 untagged
#
interface WLAN-ESS1
```

```

port link-type hybrid
port hybrid vlan 1 untagged
mac-vlan enable
#
wlan ap ap1 model WA2620E-AGN id 1
serial-id 210235A29G007C000020
radio 1
service-template 1 vlan-id 3
radio enable
#
wlan mobility-group systemgroup
member ip 192.168.1.101 vlan 3
source ip 192.168.1.100
mobility-group enable
#
dhcp enable
#

```

#### ● AC 2:

```

#
vlan 3
#
interface Vlan-interface1
ip address 192.168.1.101 255.255.255.0
#
interface Vlan-interface3
ip address 192.168.3.101 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 1 untagged
#
wlan mobility-group systemgroup
member ip 192.168.1.100 vlan 3
source ip 192.168.1.101
mobility-group enable
#

```

## 4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“WLAN 配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 命令参考”。